Recalibrating Data Retention in the EU

The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?

Adam Juszczak, Elisa Sason *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

Data retention has been subject of extensive and fierce discussions amongst practitioners, policy makers, civil society and academia in the EU and its Member States for many years – often coined as a clash between liberty and security. Through its jurisprudence, the Court of Justice of the EU ('CJEU') attempts to find a balance between the fundamental rights and freedoms at stake. This article provides a legal analysis of the jurisprudence of the CJEU on data retention, from the Decision in Digital Rights Ireland/Seitlinger to the most recent Decisions in the Cases Privacy Int., Quadrature du Net and H.K. v. Prokuratuur. It observes that while the CJEU has reconfirmed its previous jurisprudence on data retention, it widely opens the door to a variety of exceptions. The analysis covers the implications of the most recent jurisprudence of the CJEU from a legal and practical angle and seeks to establish whether, on the basis of its findings, it is indeed possible to apply these exceptions in practice. Given the link with data retention, the current state of play of the negotiations on the e-Privacy Regulation between the European Parliament, Council and Commission is briefly reflected. The article concludes that the latest jurisprudence of the CJEU does not put an end to the ongoing discussions on data retention but that there is a need for a recalibrated solution by way of a common legislative approach, at least on a set of definitions and basic notions at EU level. This could provide for the desired added value and the necessary legal certainty for all stakeholders involved, also given the increasing number of cross-border investigations and prosecutions in the EU and the fact that service providers are established all over Europe and the rest of the world.

AUTHORS

Adam Juszczak

European Commission

Elisa Sason

Policy Coordinator
European Commission

CITE THIS ARTICLE

Juszczak, A., & Sason, E. (2021). Recalibrating Data Retention in the EU : The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning? Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2021-020

Published in eucrim 2021, Vol. 16(4) pp 238 – 266

https://eucrim.eu

ISSN:

I. Introduction

Over the past years, "data retention" has been the subject of extensive, controversial and at times fierce discussions amongst practitioners, policy makers, civil society and academia in the EU and its Member States. Essentially, it is about the retention by providers of electronic communication services and networks of traffic and location data for a certain period of time, in order to allow access by competent national authorities for the purpose of preventing, investigating, detecting, or prosecuting crimes and safeguarding national security.

Although it is generally about traffic and location data and not about the content of the communication conducted, the scope of such retention remains significant. The kind of retained data enables obtaining an enormous amount of information, such as locating the source of a communication and its destination; determining the date, time, duration and type of communication; identifying the communications equipment used; locating the terminal equipment and communications; saving the names and addresses of users, the telephone numbers of the caller and the person called, and the IP address for internet services.

Data retention covers all electronic communication systems and applies to all users of such systems, not only to persons suspected of having committed a crime. It applies to all users of electronic communication, without distinction or exception.

Some repeat that it is indispensable that electronic communication operators and service providers retain certain data – besides that collected strictly for their business purposes – and disclose it, under certain conditions, to law enforcement, judicial and other competent authorities, in order to effectively prevent serious threats to security and combat serious crimes, including terrorism, organised crime or child pornography.[1] Others reiterate that such practice constitutes an invasive and unjustified encroachment on fundamental rights; they also put in question the purported benefits of the retention of data for the purpose of preventing threats and fighting crime as such.[2]

The matter of "data retention" raises myriads of legal and practical questions and touches upon fundamental rights in the European multi-level system, i.e. fundamental rights as enshrined in national constitutions (national level), and those enshrined in the EU Charter of Fundamental Rights and the European Convention on Human Rights (European level). At the EU level, the Court of Justice of the European Union (hereinafter "CJEU") as the guardian of the Charter of Fundamental Rights[3] (hereinafter "Charter"), checks whether national legislation on data retention complies with Union law, and in particular the Charter. At the same time national Supreme Courts or Constitutional Courts are competent to check compliance of national provisions against the guarantees enshrined in their national constitutions, while the European Court of Human Rights (ECtHR) reviews interferences with the European Convention on Human Rights (ECHR). This mixed and multi-layered judicial environment does not make it easy to attain clarity and certainty in establishing the scope and limits of data retention in Europe. It is hence not surprising that several national Supreme and Constitutional Courts rendered judgements on data retention in the past years,[4] as well as the ECtHR,[5] and, lastly, the CJEU.

For all the focus on the judicial and security dimension of this topic, another aspect related thereto remained out of sight: Imposing an obligation on providers of electronic communication services and networks to retain data and provide access thereto to competent national authorities, might not only potentially pose a significant financial burden on the service providers, but also comprises a considerable impact on the way they conduct their business – a right that falls under the scope of Art. 16 of the Charter. Although the CJEU

https://doi.org/10.30709/eucrim-2021-020

has reviewed the requests for preliminary ruling by referring to fundamental rights of the Charter, it has been entirely oblivious to a potential interference with said Art. 16 of the Charter.

Generally, although the protection of personal data is high on the political agenda in the EU, there has always been strong political will to find a viable solution allowing for an effective use of retained data for the purpose of combating crimes and maintaining security in the EU. The heads of state and government underlined at the meeting of the European Council in December 2020 that it is essential that national law enforcement and judicial authorities exercise their powers both online and offline to combat serious crime and – in the light of the case law of the CJEU– stressed the need to continue and advance work on retention of data in full respect of fundamental rights and freedoms[6]. At the March 2021 Justice and Home Affairs Council, Ministers, too, stressed the need for competent national authorities to have access to data previously retained for the purpose of preventing, investigating, detecting, and prosecuting serious crimes.[7]

This article provides a short background on data retention at the EU level (II.) before it outlines the most recent jurisprudence of the CJEU (III.). It subsequently elaborates on the legal and practical consequences of that jurisprudence (IV.), sheds light on this matter in the context of the current negotiations on the e-Privacy Regulation between the European Parliament, Council and Commission (V.), and concludes with a number of reflections on how and to which extent retention of personal data and access thereto could be reconciled with the requirements under EU law (VI.).

II. Quick Flash: From the Data Retention Directive to the Tele2/Watson Decision by the CJEU

At the EU level, common rules on a Union-wide data retention regime were introduced back in 2006 by Directive 2006/24/EC,[8] which obliged Member States to adopt measures to ensure that providers of electronic communication services and networks retain traffic and location data (excluding the content of the communication) for between six months and two years, in order to allow access by competent national authorities for the purpose of investigation, detection and prosecution of serious crimes.

1. Digital Rights Ireland/Seitlinger – the CJEU's decision on the invalidity of the data retention Directive

This first and somehow candid attempt to establish an EU-wide data retention regime was, to some surprise of many, declared invalid by the CJEU in 2014 in its landmark decision *Digital Rights Ireland and Seitlinger.*[9] Following legal challenges in Ireland and Austria, requests for a preliminary ruling were made by the Irish High Court and the Austrian Constitutional Court (*Verfassungsgerichtshof*), and the CJEU held that the retention of data, as envisaged in that Directive, violated Arts. 7 and 8 of the Charter. The CJEU established that the general and indiscriminate retention of data envisaged in the Directive constituted a particularly serious interference with fundamental rights, as it was not sufficiently circumscribed to ensure that the interference is limited to what was strictly necessary. However, the CJEU did not fail to stress that in its view the retention of data genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security and that, as such, it does not adversely affect the essence of the fundamental rights in question. Moreover, the CJEU stated that the Directive may be considered appropriate for attaining the objective pursued – in other words, that the retention of data and access thereto by national authorities was considered a suitable tool that indeed has an added value in combating serious crimes.[10]

Although this decision has been perceived as marking the end to data retention in the EU, the CJEU clearly did not dismiss data retention as such but the way the directive was constructed – the Union legislator failed the proportionality test. The CJEU meticulously enumerated the faulty parts of the Directive, i.e.:

- The lack of differentiation, limitation or exception when retaining all traffic data of all individuals;[11]
- The lack of any objective criteria as regards the access to the data by national authorities;[12]
- An overly rigid retention period, without any distinction as regards the categories of data and the usefulness for the objective pursued;[13]
- The absence of sufficient safeguards against the risk of abuse of the retained data;[14]
- An overly relaxed attitude allowing that the data may be retained outside the EU, hence out of reach of the required control of compliance under EU law, as also required by Art. 8(3) of the Charter.[15]

What was the immediate consequence of this decision? The CJEU declared Directive 2006/24 invalid, but it did not dismiss data retention as such, thus leaving room for national solutions, provided they comply with the standards of EU law. As the CJEU does not consider the validity of national legislation transposing that Directive, its decision could not not directly impact the domestic regimes on data retention across the EU. Although a number of national courts of last resort declared national legislation to be invalid on the basis of the *Digital Rights* decision[16] and some Member States made limited amendments, it remained unclear to which extent the findings and requirements of that decision would, in practice, impact the domestic regimes on data retention.

It required further action to bring this matter before the CJEU again and to give practical effect to the landmark judgement in *Digital Rights*. This happened just a day after the decision of the CJEU, when Swedish telecommunication company "Tele2" decided to no longer retain data and informed the Swedish authorities accordingly. Legal proceedings were instituted and, in the course thereof, the Swedish court (*Kammarrätten i Stockholm*) referred the question whether national law governing a general and indiscriminate retention of data, where the objective pursued is not limited to fighting serious crimes,[17] was compatible with Directive 2002/58/EU[18] (hereinafter "e-Privacy Directive") and the Charter. The Swedish request was joined by a UK court request, which demonstrated how innocuous the *Digital Rights* decision was perceived, when the referring court (*Court of Appeal of England & Wales (Civil Division)*) asked, whether the judgement of the CJEU in *Digital Rights* laid down mandatory requirements of EU law applicable to a Member State's domestic regime on access to data retained in accordance with national legislation.[19]

2. Tele2/Watson – the CJEU's blueprint to check invasive legislative measures on data retention and access against the e-Privacy Directive as read in light of the Charter

In its judgment of 21 December 2016, the CJEU ruled that EU law precluded national legislation that prescribed a general and indiscriminate retention of traffic and location data.[20] By building upon and reconfirming analogously the line taken in *Digital Rights,* the CJEU set out in detail its systematic approach in reviewing the compliance of national provisions with Art. 15(1) of the e-Privacy Directive in the light of Arts. 7, 8, 11 and 52(1) of the Charter. Thus, the decision *in Tele2/Watson* forms in essence the blueprint for reviewing invasive legislative measures on data retention and access thereto against the relevant Union law. Thereby, the CJEU followed a two-step approach: first, it reviews compliance of the provisions requiring the retention of data by the providers with the above-mentioned provisions, second, it reviews compliance of the

https://doi.org/10.30709/eucrim-2021-020

provisions allowing for access to that justifiably retained data by competent national authorities with said provisions of Union law.

By highlighting the high level of protection of personal data and privacy guaranteed by the e-Privacy Directive, the CJEU stressed that the principle of confidentiality enshrined in the e-Privacy Directive prohibits, as a general rule, the storage of traffic and related communication data by any person without the consent of the user.[21] Save for the technical storage necessary for the conveyance of the communication, the only exception to this rule is permitted by Art. 15(1), which enables Member States to derogate from the principle of confidentiality under certain conditions laid out therein.[22] The CJEU concluded that Art. 15(1) is to be interpreted strictly, meaning that the exception this provision allows must remain an exception and not become the rule.[23]

More concretely, the CJEU outlined that, according to Art. 15(1), Member States may adopt legislative measures derogating from the principle of confidentiality where "it is a necessary, appropriate and proportionate measure within a democratic society" to safeguard the list of objectives, i.e. national (State) security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences, or unauthorised use of the communication system. The CJEU further clarified that this list of objectives is exhaustive, and Member States cannot go beyond.[24] Moreover, it follows from Art. 15(1) that any national measure derogating from the principle of confidentiality needs to be in accordance with the general principles of EU law. This opens the avenue to checking the national legislative measures against fundamental rights enshrined in the Charter. In the same way as in *Digital Rights*, the CJEU considered the examination of the compatibility with Arts. 7, 8 and 11[25] of the Charter as pertinent. In this context, the CJEU explained that, pursuant to Art. 52(1) of the Charter, any limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law, respect the essence of those rights and be proportionate, i.e. they must be necessary and meet objectives of general interest recognised by the EU or the need to protect rights and freedoms of others.[26] These requirements are echoed in Art. 15(1) of the e-Privacy Directive, which states that data should be retained "for a limited period" and be "justified" by reference to one of the objectives mentioned in the same Article. This methodological approach is applied by the CJEU to the rules governing the retention of data (below (1)) as well as, at later stage, to those governing access to the retained data (below (2)). This is the benchmark against which the national law in question will be measured.

(1) With regard to retention, the CJEU concluded that the data retained allows very precise conclusions to be drawn concerning the private lives of the persons.[27] According to the CJEU, the fact that the persons concerned are not informed of their data being retained, is likely to cause a feeling of constant surveillance.[28] It held that the interference with Arts. 7 and 8 of the Charter was particularly serious and that only the objective of fighting serious crime was capable of justifying such serious interference.[29] The CJEU continued that even if the retained data concerns traffic and location data and not the content of communication,[30] this would have an effect on the use of means of electronic communication, and consequently, on the exercise of the user of the freedom of expression, guaranteed by Art. 11 of the Charter.[31]

In conclusion, national legislation providing for a general and indiscriminate retention of data, and where there is neither any requirement that there be a relationship between the retained data and the threat to public security, nor any other restrictions or exceptions, e.g. with regard to the time period, geographical area or group of persons, exceeds the limits of what is strictly necessary.[32] Legislation requiring such retention would in fact turn the exception envisaged in Art. 15(1) into a rule.[33]

In the same way as in *Digital Rights*, the CJEU did not dismiss data retention *per se*. Moreover, it instantly presented a possible remedy to the established disproportionality of the legislative measures under scrutiny in the case at hand: The CJEU referred to the idea of a targeted retention of traffic and location data for the purpose of serious crime. In the CJEU's view, this approach – provided it fulfils a number of strict conditions

– would be a permissive way of retaining data as a preventive measure to allow access by competent national authorities.[34] The mentioned conditions include e.g. clear and precise rules on the scope and application of the retention measure, and minimum safeguards for persons affected. The CJEU stressed that the measure must be limited to what is strictly necessary, in particular it must be based on objective evidence to identify persons, whose data is likely to reveal a link – at least an indirect one – with serious criminal offences, and to contribute to fighting serious crime or preventing a serious risk to public security. By way of an example, the CJEU mentioned a geographical criterion.

(2) With regard to access, the CJEU followed the same logic as with retention and reiterated that access to retained data must correspond genuinely and strictly to the (exhaustive list of) objectives referred to in Art. 15(1)[35] stressing that only the objective of fighting serious crime is capable of justifying access to retained data.[36] Furthermore, the CJEU recalls that legislation governing access to retained data needs to strictly comply with the proportionality principle,[37] i.e. it must not exceed the limits of what is strictly necessary. The CJEU outlined that such legislation must lay down clear and precise substantive and procedural conditions governing the access to the retained data.[38] Specifically, the legislation needs to be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities may be granted access.[39] This means that in the context of fighting crime, as a general rule, access may be granted only to the data of individuals suspected of planning, committing or having committed a serious crime or of being otherwise implicated in such crime. However, the CJEU also hinted to an exception by adding that in particular situations, where vital national interests are at stake, e.g., threats of terrorist activities, access to data of other persons might be granted, provided there is objective evidence that that data might, in a specific case (in other words, in that exceptional case), make an effective contribution to combating such activities. The CJEU nonetheless clarified that general access to all retained data, irrespective of any links or connections with the intended purpose, cannot be regarded as strictly necessary, hence it is disproportionate.[40]

The CJEU stressed that prior review by a court or an independent administrative body of the request for access by the competent authority is required, in order to ensure full respect for the necessary conditions and procedures outlined – this necessity for review also follows directly from Art. 8(3) of the Charter, although still leaving room for exceptions in urgent cases.[41] The CJEU further demanded a notification of the persons affected, once such notification no longer jeopardises the investigations undertaken.[42] In addition, the CJEU clarified that Art. 15(1) of the e-Privacy Directive does not provide for a derogation with respect to the rules relating to security and protection of the data. This requires that providers guarantee a particularly high level of protection and security, that the data is retained within the EU and that data is irreversibly destroyed at the end of the retention period.[43] Whether and to what extent the national legislation reviewed by the CJEU in *Tele2/Watson* satisfied the established requirements from Art. 15(1) read in the light of Arts. 7, 8, 11 and 52(1) of the Charter was however left for the referring court to determine. This is somehow unsatisfactory, but inevitable as the CJEU has to limit itself to its function under Art. 267 TFEU and the questions referred to it.

In *Tele2/Watson*, the CJEU ultimately shed light on the scope of the e-Privacy Directive. This has been a much-debated question and several Member States had expressed doubts as to the applicability of that Directive in the context of Member States' security measures. The CJEU held that national legislation governing the obligation of providers of electronic communication services and networks to retain traffic and location data as well as rules on access to such data by competent national authorities fall within the scope of the e-Privacy Directive, even if the sole objective of such legislation was to combat crime alone. Such legislation thus needs to be measured against the Charter.[44] The protection of the confidentiality of electronic communication and related traffic data guaranteed by that Directive applies to the measures taken by all persons (other than the users), no matter whether private persons or bodies or State bodies.[45] Legislative

measures, which, pursuant to Art. 15(1) of the e-Privacy Directive, restrict the scope of the rights and obligations provided in the e-Privacy Directive, cannot be considered "activities of the State" within the meaning of Art. 1(3) of the e-Privacy Directive, no matter if the objectives to be pursued under Art. 15(1) and the objectives referred to in Art. 1(3) overlap.[46] Referring to the structure of the e-Privacy Directive and the purpose of its Art. 15, the CJEU stressed that Member States may only adopt restrictive legislative measures, on condition that they comply with the prerequisites laid down in that very Article.[47] Accordingly, this applies to legislative measures that require providers to retain traffic and location data, as well as measures governing the access by national authorities to the retained data, since both issues include processing activities by the providers.[48] This means that the retention of data and access to such data must be considered like two sides of the same coin and both fall within the scope of the e-Privacy Directive.

3. Interim conclusion

The CJEU's jurisprudence in *Digital Rights* and *Tele2* set the threshold very high. It is a benchmark against which the CJEU is going to review later preliminary ruling requests brought on this matter. At the same time, it should be stressed that the CJEU has not dismissed data retention as such in both judgments. Even more, the CJEU considered the retention of data and access thereto by national authorities a suitable tool that has an added value in combating serious crimes, however, without specifying further how it reaches such conclusion. To that end, the CJEU left room for possible forms of data retention from the beginning, giving ample advice on what such solutions could look like.

At the same time, despite the clear language of the CJEU in *Digital Rights* and *Tele2*, there was no coherent understanding at the national level as to how these judgements and their consequences should be interpreted. At least, there seemed room for interpretation. In 2017, for instance, the Constitutional Court of Portugal found that the declaration of invalidity of the data retention Directive did not have an automatic consequence on the validity of a national law transposing it. Moreover, it found that Portugal introduced an extensive and complex framework, including on access to and protection of retained data, which goes far beyond the invalid data retention Directive and the CJEU's jurisprudence, and that these specificities have to be looked at in their entirety and could not be disregarded when assessing certain provisions on data retention. The Constitutional Court of Portugal hence declared the retention of subscriber information with respect to dynamic IP addresses on the basis of the Portuguese Law as constitutional.[49] The Council of Ministers of Belgium argued a year later in a similar way in proceedings before the Constitutional Court (*Cour Constitutionelle*) of Belgium.[50]

Overall, a large number of Member States did not see a compelling need to fundamentally change their national laws and, in effect, the previous practice remained in place as before.

III. Recalibrating Data Retention in the EU. The CJEU's Decisions in the Cases *Privacy Int.*, *Quadrature du Net* and *H.K. v. Prokuratuur*

Following the *Tele2* decision, the rules governing the activities of national intelligence agencies came more and more into the focus of national courts in several Member States. Although the CJEU in *Tele2* also scrutinised the Swedish Law on gathering of data relating to electronic communication as part of intelligence gathering by law enforcement authorities,[51] national courts generally expressed doubts that the strict line taken by the CJEU in its previous decisions with regard to the retention of data and the access thereto could be applied to the sensitive activities of national intelligence agencies. Requests for preliminary ruling were

thus made by the Investigatory Powers Tribunal in the United Kingdom,[52] the French Conseil d'Etat[53] and the Belgian *Cour Constitutionelle*[54], which the CJEU took a stance on in two comprehensive judgements of 6 October 2020. Shortly thereafter on 2 March 2021, the CJEU shed more light on this matter in a request for preliminary ruling submitted by the Supreme Court of Estonia.[55]

1. Facts of the cases in Privacy Int., Quadrature du Net, *Ordre des barreaux francophones and germanophone* et. al.

The UK request in the case *Privacy International* concerned the transfer of bulk communication data from providers of public communications networks, under the directions issued by the UK Secretary of State, to national security and intelligence agencies, where that data was used by those agencies, in particular by way of automated processing. This practice is said to have been going on for almost two decades. The referring court highlighted the importance of using bulk communication data by security and intelligence agencies for the protection of national security, including counter-terrorism, counter-espionage and counter-nuclear proliferation, and found that this practice was also compliant with the ECHR. It hence sought to clarify whether, and if so to what extent, EU law and in particular the e-Privacy Directive, was applicable, given that according to Art. 4(2) TEU and in view of Art. 1(3) of the e-Privacy Directive, national security remains the sole responsibility of the Member States.[56]

The French and Belgian requests in *Quadrature du Net et. al.* and *Ordre des barreaux francophones and germanophone and Others* concerned a wide range of questions surrounding the newly adopted data retention regimes in place in France[57] and Belgium[58] respectively.

The Belgian legislation envisaged a general and indiscriminate retention of traffic and location data for a period of 12 months and allowing access thereto by various national authorities, e.g., police and judicial authorities, intelligence and security authorities as well as emergency call services and authorities responsible for missing persons. The motifs of that legislation state that it is impossible to know in advance which data is needed and that it is equally impossible to limit the retention of data to certain groups of persons, to include time limits or to restrict the retention to geographic areas.[59] In the proceedings before the *Cour Constitutionelle* it was even stated that a "targeted retention", as suggested by the CJEU in *Tele2*, could easily lead to or be perceived as discrimination.[60] The Belgian Constitutional Court hence asked, first, whether a general data retention obligation, which is provided with certain safeguards on storage and access, was compatible with EU law and in particular Art. 15(1) of the e-Privacy Directive and Arts. 7, 8 and 52(1) of the Charter, taking into account that the aim of the legislation was not limited to fighting serious crime but also intended to safeguard national security, defence, public security, and to prevent, investigate, detect and prosecute other criminal offences. The Belgian Constitutional Court then reverses the perspective and asks in its second question whether general data retention may be duly justified if the objective is to enable the state to fulfil its positive obligations under Arts. 4 and 7 of the Charter, thus, ensuring the effective criminal investigation and effective punishment of perpetrators of sexual abuse of minors, when they made use of electronic communication means. The Constitutional Court finally asks whether, in the event that the CJEU finds the data retention legislation under review as incompliant with EU law, the consequences of that legislation could be maintained, in order to enable the further use of previously stored data, so as to avoid legal uncertainty.

Similarly, the French requests concerned legislation adopted after the *Charlie Hebdo* and *Bataclan* terrorist attacks. The legislation envisaged gathering intelligence related to protecting and promoting a set of State interests, such as national independence, integrity, defence, and prevention of terrorism or organised crime as well as certain foreign policy, economic, industrial and scientific interests. The referring French court sought clarity as to whether a general and indiscriminate retention for such purposes may be justified by the

right to security guaranteed by Art. 6 of the Charter, thereby also highlighting that national security falls within the sole responsibility of the Member States pursuant to Art. 4(2) TEU. It also inquired about the compliance with EU law of special measures for the purpose of preventing terrorism, such as real-time collection of traffic and location data and automated data processing, which, as the referring court noted, would not impose any specific retention obligations on the providers of communication and network services. The referring court lastly sought clarity in relation to the collection of metadata, namely whether it is a prerequisite for the collection that the data subjects are notified of the measures.

2. Key findings of the CJEU

In the judgments deciding the three cases, the CJEU generally follows the line of argument taken in its previous decisions. However, it also opened the door to a number of important exceptions in very elaborate and concrete terms. If one were to sum up the previous decisions as to say that data retention was overall prohibited unless it is allowed in certain situations, the impression now is that data retention may be more widely used, as long as it is not excessive (in particular if one reads the *Quadrature du Net* judgment). The following analyses in detail the judgments in *Privacy Int.* and *Quadrature du Net* et al. underpinning this hypothesis.

a) Clarifying the scope of the e-Privacy Directive

At first, the CJEU reconfirmed its established argument taken in *Tele2* regarding the scope of the e-Privacy Directive. National measures do not fall outside the scope of the Directive just because they have been taken for the purpose of protecting national security.[61] The CJEU stressed that such measures need to comply with the prerequisites laid down in Art. 15(1), both, in respect of retaining data as well as access thereto and cannot be considered "activities of the State" within the meaning of Art. 1(3), no matter if the objectives to be pursued under Art. 15(1) and the objectives referred to in Art. 1(3) of the e-Privacy Directive overlap.[62]

Art. 4(2) TEU does not change this conclusion. The CJEU acknowledged, in line with its earlier jurisprudence, that it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security.[63] However, it holds that the mere fact that a national measure has the purpose of protecting national security cannot render EU law, such as the e-Privacy Directive, inapplicable and exempt the Member States from their obligation to comply with that law.[64] These findings also apply to the special case of the UK request, where the CJEU dismissed the argument that the transfer of the entire data to intelligence authorities by the service and network providers was to be considered mere technical assistance to an act carried out solely by the State to protect national security, as stipulated in Art. 4(2) TEU.[65]

The CJEU also clarified that nothing else follows from its judgement in Case *Parliament v. Council and Commission,*[66] where the CJEU held in the context of Passenger Name Records (PNR) that the transfer of personal data by airlines to the public authorities of a third country for the purpose of preventing and combating terrorism and other serious crimes fell outside the scope of the data protection Directive 95/46.[67] Although Art. 1(3) of the e-Privacy Directive, which excludes from the scope of that directive, in a similar manner as Art. 3(2) of Directive 95/46 did in the past, activities concerning public security, defence and State security, the comparison with the case on PNR does not hold in the CJEU's view. According to the CJEU, the wording of Art. 3(2) of Directive 95/46, was broader and excluded in a general way processing operations concerning public security, defence and State security from its scope, regardless of who is carrying out the data processing operations. [68] By contrast, Art. 1(3) of the e-Privacy Directive, as the CJEU points out, makes a distinction as to who carries out the data processing operation concerned with all processing operations by

providers of communication services, including processing operations resulting from obligations imposed by the public authorities, falling within the scope of the e-Privacy Directive.[69]

Moreover, Directive 95/46 was repealed by Regulation 2018/679 (the General Data Protection Regulation – hereinafter "GDPR") and although Art. 2(2)(d) GDPR envisages that processing operations by "competent authorities" for the purpose of, *inter alia*, prevention and detection of criminal offences are not covered by that Regulation, Art. 23(1)(d) and (h) GDPR makes it clear that processing of personal data carried out by individuals clearly falls within the scope of that Regulation. The interpretation of the e-Privacy Directive, which supplements and further specifies the GDPR, is insofar consistent.[70] The CJEU states that only measures that are directly implemented by national authorities fall outside the scope of the e-Privacy Directive and have to be assessed on the basis of national (constitutional) law and the ECHR.[71]

Overall, the CJEU follows a narrow interpretation of Art. 4(2) TEU, which does not leave much room outside the scope of EU law. The CJEU draws a very fine line between its judgement on *PNR* on the one hand and its judgements in *Privacy International* and *Quadrature du Net* on the other. The CJEU did not (have to) elaborate in its *PNR* decision on the differences in the wording and the scope of Art. 3(2) of Directive 95/46 and Art. 1(3) of the e-Privacy Directive, respectively; this point was highlighted only later in the *Quadrature du Net* decision, more concretely, in the opinion provided by Advocate General Campos Sánchez-Bordona.[72] In its *PNR* decision, the CJEU essentially based its findings on the point that although the PNR data was collected by private operators for commercial purposes and subsequently transferred by them to a third country, Art. 3(2) of Directive 95/46 still applied and (hence) that the actual transfer of data fell outside the scope of that Directive. The transfer fell, instead, within a framework established by the public authorities that related to public security.[73] It begs the question whether the CJEU would indeed have decided on *PNR* today in the same way as it did in 2006, in view of its approach it has taken most recently.

b) Reconfirming the preclusion of a general and indiscriminate retention of traffic and location data

The CJEU then reconfirmed its established line that EU law precludes national legislation that prescribes a general and indiscriminate retention as well as a transmission of traffic and location data.[74] This also applies in respect of security and intelligence agencies for the purpose of safeguarding national security.[75] Thereby, the CJEU closely followed its systematic approach developed in *Tele2*. It reiterated the principle of confidentiality of traffic and location data protected under the e-Privacy Directive and the safeguards, which apply in the case of an exceptional derogation based on Art. 15(1), in particular the strict compliance with the rights enshrined in the Charter. The CJEU identified Arts. 7, 8 and 11 of the Charter as the fundamental rights affected, without actually defining in detail the scope of protection of these rights. The CJEU pointed out, however, that the protection under the e-Privacy Directive directly emanates from the rights enshrined in Arts. 7 and 8 of the Charter.[76]

It stressed that the retention in itself constitutes an interference with those fundamental rights, irrespective of whether such data is sensitive, harmful to the persons concerned or whether such data has actually been used subsequently.[77] It also flagged the potential risks of abuse and unlawful access resulting from the significant quantity of traffic and location data retained under a general and indiscriminate retention measure.[78] In line with Art. 52(1) of the Charter, the CJEU examined whether, and if so to what extent, the limitations on the fundamental rights affected caused by the measures under review are justified, in particular, whether such measures are proportionate and meet the objectives of general interests recognised by the Union or the need to protect the rights and freedoms of others.

Accordingly, the CJEU turned to the question, as specifically requested by the referring courts, whether any positive obligations flowing from Arts. 3, 4, 6 and 7 of the Charter, could demand the adoption of measures,

such as those under review, which could be in conflict with Arts. 7, 8 and 11 of the Charter and accordingly Art. 15(1) of the e-Privacy Directive in the present cases.

With regard to the right to security of person in Art. 6 of the Charter, the CJEU makes reference to the ECtHR case law on the corresponding Art. 5 ECHR.[79] The CJEU clearly dismissed the idea put forward by the referring courts that Art. 6 of the Charter could impose any sort of positive obligations on the State to take specific measures to prevent and punish certain criminal offences,[80] which would justify the derogation from the principle of confidentiality under the e-Privacy Directive.

The CJEU was however more susceptible to potential positive obligations deriving from Art. 3 (right to the integrity of the person), Art. 4 (prohibition of torture and inhuman or degrading treatment or punishment), and Art. 7 (respect for private and family life) of the Charter.[81] Without defining the scope of application and the width of these rights, the CJEU just made reference to the jurisprudence of the ECtHR on Arts. 3 and 8 ECHR, which correspond to Arts. 4 and 7 of the Charter, and stated that the rights require the putting in place of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against a person through effective investigation and prosecution – this in particular, when a child's physical and moral well-being is at risk.[82] To that end, the CJEU concluded that, as the ECtHR found, a legal framework should be established allowing to strike a balance between the various interests and rights to be protected.[83] The CJEU did, however, not go into greater detail or elaborate on the scope of any of these positive obligations and to what extent they themself are subject to limitations.

With regard to proportionality, the CJEU reiterated that derogations from and limitations on the protection of personal data must apply only insofar as they are strictly necessary and that the objective pursued must be proportionate to the seriousness of the interference.[84] This requires the laying down of clear and precise rules on the scope and application of the measure in question and ensuring minimum safeguards. In particular, the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued.[85]

c) Recalibrating data retention – exceptions to the strict rule followed by the CJEU hitherto

While the CJEU in *Tele2* opened a crack in the door for a data retention regime that would satisfy the CJEU's strict requirements by introducing the concept of a "targeted retention", it now widely opened the door in the *Quadrature du Net* decision for a variety of possible exceptions to its established rule that a general and indiscriminate retention of traffic and location data is precluded. Building on the approach, line of arguments and caveats developed in *Tele2*, the CJEU underlined that the different objectives referred to in Art. 15(1) of Directive 2002/58 as well as the types of personal data demand differentiation as regards the potential limitations to the principle of confidentiality of personal data. Moreover, there is a need to strike a balance between the rights and the interests at issue depending on the circumstances of the case. The CJEU elaborated on the various types of scenarios and exceptions, one by one:

aa) Legislative measures for the purpose of safeguarding national security

The first and presumably the most far-reaching and significant exception concerns measures providing for the preventive retention of traffic and locations data for the purpose of safeguarding national security. The CJEU stressed that the objective of safeguarding national security has not yet been specifically examined by it, although it already clearly hinted to a different treatment of measures for the purpose of safeguarding national security in particular situations in *Tele2*.[86]

Briefly and without much ado, the CJEU went back to Art. 4(2) TEU – which it dealt with in detail in the context of reviewing the scope of application of EU law for measures that serve the purpose of protecting

national security (see above a)). It now recalls that national security remained the sole responsibility of Member States and that that responsibility corresponds to the primary interest to protect the essential functions of the State and the fundamental interests of the society. This responsibility entails the ability to prevent and punish activities which could seriously go against these interests. By way of an example the CJEU mentioned terrorist activities.[87] As already pointed out in *Tele2,*[88] the CJEU set out that the objective of safeguarding national security is different from the other objectives referred to in Art. 15(1) of the e-Privacy Directive. Outlining that threats to national security are different by their nature and particularly serious, the CJEU concluded that the objective of safeguarding national security is hence capable of justifying measures that entail a more serious interference with fundamental rights, provided that the other requirements as laid down in Art. 52(1) of the Charter are met.[89] To this end, the CJEU did not mention any potential positive obligations that could be derived from the fundamental rights that the CJEU itself had identified in this context and that could potentially demand justifying such exception.

On that basis, the CJEU concluded that, as long as there are sufficiently solid grounds that a Member State is confronted with a serious threat to national security, which is genuine and present or foreseeable, Art. 15(1) of the e-Privacy Directive read in light of the Charter does not preclude legislative measures which permit ordering the providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time. Although the CJEU still echoed the principles it had established in its previous jurisprudence, such as that the instruction to retain must be limited in time to what is strictly necessary, it clarified that the instruction may be renewed for a foreseeable period of time, however, stressing that the retention cannot be systematic in nature. To that end, the instructions to providers of electronic communications services have to be subject to effective review by a court or an independent administrative body, which needs to verify that one of the situations justifying the general and indiscriminate retention actually exists and that the conditions and safeguards are observed.[90]

bb) Legislative measures for the purpose of safeguarding public security (criminal offences)

As regards legislative measures for the purpose of safeguarding public security, that is preventing, investigating, detecting and prosecuting criminal offences, the CJEU followed its systematic approach in *Tele2* (see above); however, it shed more light on possible exceptions, in particular on its concept of "targeted retention". It reiterated that, based on the principle of proportionality, only the objective of fighting serious crime and measures to prevent serious threats to public security are capable of justifying an interference such as the retention of traffic and location data. The CJEU clarified that even positive obligations, which might flow from Arts. 3, 4, and 7 of the Charter, as outlined above, cannot justify an interference that is as serious as the retention of traffic and location data without any restrictions and without a connection between the data of the persons concerned and the objective pursued.

This is different, as the CJEU pointed out, in the case of a "targeted retention", provided it is designed in a way that the legislation envisaging the retention of traffic and location data is limited to what is strictly necessary with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted. The choice must be based on objective and non-discriminatory factors.[91] The CJEU also considered that a targeted retention for the purpose of combating serious crimes or preventing serious threats to public security would be justified, *a fortiori*, for the purpose of safeguarding national security. In other words, what suffices for the less serious purpose, also suffices for the graver one.

cc) Preventive retention of IP addresses and data relating to civil identity to combat crime and safeguarding public security

The third exception concerns, in essence, ways and means to identify the users of electronic communications systems, i.e. the retention of IP addresses and data relating to civil identity. The CJEU stated that IP addresses mainly help identify the natural person who owns the device from which an internet communication is made.[92] Provided that only IP addresses of the source and not the IP addresses of the recipient of the communication are retained, the CJEU considered this category of data as being less sensitive than other traffic data.[93]

Nonetheless, since IP addresses may be also used, beyond determining the terminal equipment utilised, to track the user's clickstream, thus, the entire online activity and hence establish a detailed profile of the user, the retention would constitute a serious interference with Arts. 7, 8 and 11 of the Charter.[94] The CJEU noted, however, that for the detection of criminal offences committed online, the IP address might be the only possibility to identify the person to whom that IP address was assigned at the time of the commission of the offence. Without retaining the IP address, the detection of offences committed online - the CJEU specifically mentioned serious child pornography offences in this context - may prove impossible.[95]

The CJEU conceded that a retention of IP addresses of all natural persons who own terminal equipment permitting access to the internet would include also those, who "at first sight"[96] have no connection with the objectives pursued.[97] Notwithstanding, the CJEU concluded that "in those circumstances"[98] the general and indiscriminate retention of IP addresses assigned to the source of a connection does not, in principle, appear to be contrary to Art. 15(1) of the e-Privacy Directive read in light of the Charter – provided that it is subject to strict compliance with substantive and procedural conditions. This means that such retention may be only used to combat serious crimes or to prevent serious threats to public security – and *a fortiori* also to safeguard national security. The retention period must not exceed what is strictly necessary, while conditions and safeguards on the use of the data, particularly as regards tracking, need to be in place and strictly objective.

In the same context, the CJEU reconfirmed its previous jurisprudence as regards data relating to the civil identity of users of electronic communication systems and developed its approach further. It maintained its line that such data only provides contact details of the user, such as the name and the address, and that it neither concerns the date, time, duration or frequency of the communication, nor the recipients of the communication or the location where the communication took place. The CJEU held that data relating to the civil identity does not contain any information on the communications sent and hence on the user's private life.[99] Although the retention of such data constitutes an interference with Arts. 7 and 8 of the Charter, this interference cannot be considered to be serious, according to the CJEU. Thus, such non-serious interference may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general.[100] While in *Ministerio Fiscal*[101] the CJEU only ruled on the question of access to such data,[102] it looked in *Quadrature du Net* at the question of the retention of such data in itself and concluded, after striking a balance between the conflicting interests,[103] that Art. 15(1) of the e-Privacy Directive read in the light of the Charter does not preclude legislative measures requiring providers of electronic communication services to retain data relating to the civil identity of all users for the purpose of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security. Although such retention may be justified with the objective of preventing or combating any criminal offence,[104] the CJEU held that there is not even a necessity for a connection between the retained data on civil identity of all the users and the objectives pursued.[105] Furthermore, the CJEU stated that there is no specific time limit for such retention,[106] while it remained entirely silent on the question of judicial review.

dd) Legislative measures providing the expedited retention of traffic and location data for the purpose of combating serious crime ("quick freeze")

The next exception concerns cases of expedited retention of traffic and location data for the purpose of combating serious crime, sometimes also referred to as "quick freeze". In these situations, the data has been already stored by the service providers, *e.g.* for billing, traffic management or value added services.[107] As that data needs to be erased or made anonymous after a certain period of time to comply with the principle that the storage does not exceed the limit of what is strictly necessary, competent authorities may order an expedited preservation of such data in order to preserve it for the purpose of investigating criminal offences or acts adversely affecting national security. This is pertinent, according to the CJEU, only in situations, where these offences or acts have been already established or where such offences and acts may reasonably be suspected.[108] The CJEU referred to the Council of Europe Convention on Cybercrime,[109] which envisages the adoption of measures, such as the expedited preservation of traffic data, for the purpose of criminal investigations, where there are grounds to believe that that data may be lost or modified.[110]

Given the serious interference with fundamental rights, which such retention would entail, only actions to fight serious crime and, *a fortiori*, safeguarding national security may be justified.[111] Moreover, when balancing the rights and interests at issue, the CJEU stressed that under Art. 8(2) of the Charter the processing of data must be consistent with its specified purpose, while the purpose for retaining data in the case of the expedited retention (fighting crime) might not or no longer correspond to the purpose for which the data was initially processed and stored (e.g. billing). The CJEU held that it is permissible to adopt legislation under Art. 15(1) of the e-Privacy Directive, which provides for the possibility of an expedited retention, whereby competent authorities[112] may instruct providers of electronic communication services to undertake an expedited retention of traffic and location data for a specified period of time.[113] However, such legislation must clearly set out for what purpose such expedited retention may be requested, while the instruction decision shall be subject to judicial review.[114] To comply with the principle of proportionality, the retention must relate only to traffic and location data that may shed light on serious crimes or acts affecting national security, while the retention period must be limited to what is strictly necessary (however, if necessary, the retention period may also be extended).[115] Despite the limitation to what is strictly necessary, this leaves some interpretative room; the CJEU further widened the scope of this exception by stating that the data does not need to be limited to the persons specifically suspected of the crimes or the act in question but also to other persons or geographic areas, provided that on the basis of objective and non-discriminatory factors such data can shed light on the offences or acts in question.[116] It is of particular note that, according to the CJEU, the exception of an expedited retention may be combined with another exception justified under Art. 15(1) of the e-Privacy Directive, e.g. in situations where the time period of a measure is due to expire that data may be preserved beyond that period by way of the expedited retention. This opens up for a great degree of flexibility and wider use of the measures under Art. 15(1).[117] Access to such data is granted following the general principles on access, as established in *Tele2*.[118]

ee) Legislative measures providing for an automated analysis and real-time collection of traffic and location data for the sole purpose of preventing terrorist activities

Beyond the general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security, which the CJEU exceptionally considered justified under certain strict conditions,[119] it also had to review legislation that concerned certain preventive intelligence gathering techniques used in situations of serious threats to national security: the automated analysis and real-time collection of traffic and location data, as well as the real-time collection and transmission of technical data concerning the location of terminal equipment.

The automated analysis envisages a screening at the request of competent national authorities of all traffic and location data carried out by providers of electronic communication services against previously set parameters.[120] This covers all traffic and location data of all users of electronic communication systems and constitutes a processing of data with the assistance of an automated operation within the meaning of Art. 4(2) GDPR.[121] This processing is also independent of the subsequent collection of data of persons identified following the automated analysis. The CJEU pointed out that this intelligence gathering technique is likely to reveal the nature of the information consulted online and is conceived so as to apply generally to all persons, including to those, where there is no evidence that their conduct is linked in any way with terrorist activities. The CJEU concluded that this processing constitutes a particularly serious interference with Arts. 7, 8 and 11 of the Charter.

To justify such particularly serious interference in accordance with Art. 52(1) of the Charter, the CJEU fetched the requirements it established in the context of the legislative measures for the purpose of safeguarding national security (see above), stressing that the automated analysis of traffic and location data may only be considered as proportional in situations in which a Member State is facing a serious threat to national security which is genuine and present or foreseeable and provided that the duration is limited to what is strictly necessary.[122] The decision authorising automated analysis must be subject to review by a court or an independent administrative body, which verifies whether the situation justifying that measure exists and whether the conditions and safeguards that must be laid down by legislation are observed.[123] Given the specificities of the automated analysis, the underlying models and criteria for the automated analysis must be determined in a non-discriminatory manner,[124] and any positive result obtained from such analysis requires an individual re-examination by non-automated means before the person concerned is adversely affected by a subsequent measure, such as a real-time collection of his/her traffic and location data.[125] Generally, the CJEU saw a need for regular re-examinations of the pre-established models and criteria to ensure that they are up-to-date and non-discriminatory and limited to what is strictly necessary.[126] The CJEU left open who should carry out such examination and at which frequency.

The CJEU's review of the real-time collection of traffic and location data generally builds upon the automated analysis. It may be individually authorised in respect of a person or persons belonging to the same circle previously identified through the automated analysis as potentially having links to a terrorist threat.[127] Such processing allows for continuous monitoring and in real-time – for the period of time authorised – of the person(s), the means and duration of communication, the place of residence and movements of that/these person(s) and may also reveal the information consulted online. The legislation under review in *Quadrature du Net* envisaged also the possibility to collect the technical data concerning the location of the device used and transmit it in real-time to a department reporting to the Prime Minister.[128]

The CJEU noted that such measure constitutes a derogation from Art. 15(1) of the e-Privacy Directive and an interference with Arts. 7, 8, and 11 of the Charter, stressing that the real-time collection and transmission of data that allows a real-time location of the device used is particularly serious, amounting to virtually a total monitoring of the persons(s) concerned. Such real-time access is more intrusive than a non-real-time access.[129]

The CJEU held that this measure, which aims at preventing terrorist activities, and which complements the automated analysis and the exceptional general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security (see above), may be justified only in respect of persons for whom there is a "valid reason to suspect" that they are involved "in one way or another in terrorist activities."[130] Persons, who do not fall into this category, e.g., who are potentially involved in serious crimes but not terrorist activities, might fall into one of the other exceptions described by the CJEU (see above).

The decision authorising such real-time collection must be based on objective and non-discriminatory criteria provided for in national legislation. It must be subject to prior review by a court or an independent administrative body, which needs to check whether the conditions are observed, in particular whether the real-time collection is limited to what is strictly necessary.[131]

In this context, the question arose whether the person(s) concerned by these intelligence gathering measures need to be notified and whether such notification is a prerequisite for the compliance with the requirements under Art. 15(1) of the e-Privacy Directive.[132] The French law in question did not envisage a notification. Instead, it provided for the possibility for any person to file a complaint with the Commission for the Oversight of Intelligence Techniques; this Commission verified that no intelligence techniques have been unlawfully implemented against the complainant.[133] The Commission subsequently notified the complainant that it assessed the complaint, however, it neither confirmed nor denied that an intelligence gathering technique was applied against the complainant.[134] The complainant then could seek recourse before a special panel of the *Conseil d'Etat*, which investigated the complaint and, could request the competent authorities to remedy illegalities found.[135] According to the referring French court, this complaint mechanism satisfied the requirements under Art. 15(1) read in light of the Charter.[136]

Contrary to the views expressed by the referring French court, the CJEU held that the person affected by a real-time collection of traffic and location data needs to be notified.[137] This is necessary to enable the person to exercise his/her rights under Arts. 7 and 8 of the Charter, *i.e.* to request access to the data that has been subject of the measures and to request rectification or erasure, if necessary.[138] The requirement to notify also follows from Art. 47 of the Charter, which guarantees the right to an effective remedy before a tribunal, a right explicitly mentioned in Art. 15(2) of the e-Privacy Directive, read in conjunction with Art. 79(1) GDPR.[139] As for the automated analysis, which is applied generally to all persons, the CJEU held that the competent national authority needs to publish information of a general nature relating to the analysis, without having to notify each and every person individually. However, once a person has been identified on the basis of the models and criteria of the automated analysis, it is necessary to notify that person individually. The CJEU stressed, however, that the notification must take place only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which the authorities are responsible.[140]

d) Access by competent national authorities

In its recent decisions, the CJEU mainly elaborated on the various exceptions it established as far as the retention of traffic and location data is concerned. As regards an authority's access to such data, the CJEU primarily reiterates its findings in *Tele2* (see above II.); however, it also provides greater clarity on its jurisprudence and develops it further.

aa) Greater clarity on the CJEU's strict line on access to retained data

Alas, following the line taken in *Tele2*, the CJEU stressed that access may be justified only by the public interest objective, for which the providers were ordered to retain the data, and must comply with the principle of proportionality.[141] To dispel any doubts, the CJEU stressed in particular that access to data for the purpose of prosecuting and punishing an ordinary criminal offence may not in any event be granted where the retention of that data has been justified by the objective of combating serious crime or safeguarding national security.[142] However, similarly as for the retention for the purpose of combating crime and safeguarding public security, the CJEU followed the logic that what suffices for the less serious purpose, also suffices for the graver one. This means that access to data, which was retained for the purpose of serious crime, may also be justified if access is sought for the purpose of safeguarding national security.[143]

This underlines the independence of and inter-dependence between the retention and the subsequent access thereto – independence because the CJEU checks the validity of the retention and the access for each independently and inter-dependence because both are linked with and have an impact on each other.

Generally, as outlined in *Tele2,* prior review by a court or an independent administrative body of the reasoned request for access by the competent authority is mandatory in order to ensure full respect of the necessary conditions and procedures outlined.[144]

The CJEU also shed more light on cases of duly justified urgency, where it holds that the review by a court or independent administrative body needs to take place quickly but not necessarily before accessing the data.[145] The CJEU, however, did not elaborate in greater detail on what constitutes such due justification and how access should be granted in the absence of a prior (authorising) decision.

Finally, the CJEU also clarified that these requirements also apply to the particularly invasive automated analysis and real-time collection of traffic and location data;[146] in particular, a court or an independent administrative body needs to check whether the conditions are fulfilled, and the measure is limited to what is strictly necessary.

bb) Proportionality considerations on access and flawed retention – case HK v Prokuratuur

The inter-dependence between retention and subsequent access to traffic and location data, referred to above under aa) was also illustrative in the CJEU's most recent decision on a request for preliminary ruling by the Supreme Court of Estonia.[147] This request concerned criminal proceedings against a person found guilty of the commission of petty crimes and acts of violence,[148] where the question arose whether Art. 15(1) of Directive 2002/58 read in light of the Charter precludes national legislation that permits public authorities to obtain access to a set of traffic and location data for the purpose of preventing, investigating, detecting, and prosecuting criminal offences that were not limited to serious crimes, even if the access granted was short and the type of data accessed limited. The Estonian legislation in question envisaged a general and indiscriminate retention of traffic and location data related to fixed and mobile telephony for one year. Access thereto could be requested in relation to any type of criminal offence.[149] The data obtained in such way was constitutive for the conviction in the main trial in the case at issue.

The CJEU reiterated that access may be granted only insofar as the data was retained in a manner consistent with Art. 15(1),[150] thereby referring to its jurisprudence on the preclusion of a general and indiscriminate retention of traffic and location data.[151] In that sense, access may be justified only by the public interest objective for which the providers of electronic communication services were ordered to retain the data[152] and provided it is proportionate to the seriousness of the interference with Art.15(1) of Directive 2002/58 read in light of Arts. 7, 8 and 11 of the Charter.[153]As outlined in its earlier jurisprudence, the CJEU stressed that only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying a serious interference with fundamental rights, such as the retention of traffic and location data, no matter whether the retention is general and indiscriminate – as in the case under review – or targeted.[154]

Accordingly, access to a set of traffic and location data is justified only by the objective of combatting serious crime or prevent serious threats to public security.[155] The CJEU clarified that nothing changes if account is taken of factors related to the proportionality of the request for access, such as the length of the period in respect of which access to such data is sought or a narrow scope of the categories of data covered, because these factors cannot justify from the outset that access is granted in pursuance of the objective of preventing, investigating, detecting and prosecuting criminal offences in general.[156] The interference with fundamental rights in the case under review is and remains serious which may be only justified by

pursuing the objective to prevent or investigate serious crimes, rather than crimes in general. In the case at issue, the access failed already at the first step, while subsequent considerations of the proportionality of the access are insofar irrelevant.

cc) What does (not) constitute a court or independent administrative body?

In *HK v Prokuratur*, the CJEU ultimately had to take a stance on the question of what constitutes a "court or independent administrative body" within the meaning of its jurisprudence on data retention. The question was whether Art. 15(1) of the e-Privacy Directive read in light of the Charter precludes national legislation that confers on the public prosecutor's office the power to authorise access to traffic and location data for the purpose of criminal investigations.[157] The referring Estonian Supreme Court stated that, under national law, the public prosecutor's office, which is hierarchically organised, is obliged to act independently and is subject only to the law. It examines incriminating and exculpatory evidence in the pre-trial procedure and represents the public prosecution at the main trial, thus it is a party to the proceedings. There are, however, no formal requirements to access the desired data and, in effect, the prosecutor may make a request for access himself in a case.[158]

It is not surprising that the CJEU set an end to this practice. It recalls that national legislation adopted pursuant to Art. 15(1) needs to lay down the substantive and procedural conditions governing the access by the competent national authorities to traffic and location data retained by providers of electronic communications services and must comply with the principle of proportionality.[159] Such legislation must provide for clear, precise and objective rules governing the scope and application of the measure and impose minimum safeguards to effectively protect against the risk of abuse. Above all, a general access to all retained data cannot be regarded as being limited to what is strictly necessary.[160]

The court or an independent administrative body entrusted to carry out the review of the reasoned request for access must have all the power and provide all the necessary guarantees to reconcile the various interests and rights at issue.[161] The CJEU indicated that the independent administrative body must have the status enabling it to act objectively and impartially when carrying out its duties and must be free from any external influence.[162] The requirement of independence of the court or body means that it has to be different from the authority that makes the request in order to review the matter objectively and impartially and free from any external influence. This means in particular that the court or body must not be involved in the conduct of the criminal investigations in question and has to be neutral vis-à-vis the parties to the criminal proceedings. These requirements are not fulfilled in the case of a public prosecution office, irrespective of its independent status under national law.[163] Although not congruent, it is to be seen how this jurisprudence will be reconciled with the CJEU's jurisprudence on the status of a public prosecution office as a judicial authority for the purpose of issuing European Arrest Warrants.

e) Consequences of a potentially unlawful retention of or access to data used as evidence in criminal proceedings

Having elaborated extensively on the various rules and exceptions of a data retention regime, the CJEU had to address the question on the consequences of a potential unlawful retention of or access to traffic and location data that was used as evidence in criminal proceedings. This question was put forward by the Belgian *Cour Constitutionelle*.[164] Concretely, the referring Belgian court sought to address that issue by inquiring whether it may maintain the effects – at least temporarily – of the national law on data retention under review, even if the CJEU has found that it does not comply with EU law.[165] The *Cour Constitutionelle* states that maintaining the effects would allow national authorities to continue using the previously collected and retained data, primarily for the purpose of criminal proceedings, thus avoid legal uncertainty.[166] This would mean that legislation would continue to impose obligations on providers of electronic communications

services which are contrary to EU law, and which seriously interfere with fundamental rights of the persons whose data had been retained.

The CJEU unequivocally dismissed this possibility and clarified that only the CJEU may allow the temporary suspension of a rule of EU law with respect to national law that is contrary thereto. This is about primacy and uniform application of EU law – which would be undermined, if national courts were to give provisions of national law primacy over EU law, even only temporarily.[167]

As regards the question of what this means for criminal proceedings in which information and evidence obtained by a retention of data contrary to EU law was or is being used, the CJEU held that it is, in principle, for national law alone to determine rules on the admissibility and evaluation of such obtained information and evidence.[168] In the absence of EU rules on that matter, it is, in accordance with the principle of procedural autonomy, for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights that individuals derive from EU law.[169] However, Member States are not entirely free in doing so, as they need to ensure that these national rules comply with the principle of equivalence and the principle of effectiveness, i.e. that they are not less favourable than rules governing similar domestic situations and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law.[170] It is for the competent national court in criminal proceedings to ensure that these principles are safeguarded. However, the CJEU pointed out that it does not follow from the principle of effectiveness that unlawfully obtained information and evidence used in proceedings against a person suspected of the commission of criminal offences needs to be prohibited as such. For, other means may, too, serve the purpose of not prejudicing that person unduly by using unlawfully obtained material, such as national rules and practices governing the assessment and weighting of such information and evidence or the consideration whether such material is determining the sentence.[171]

The CJEU stressed that in deciding whether to exclude such information and evidence the competent national court needs to give particular attention to the adversarial principle, hence the right to a fair trial.[172] Accordingly, the right to a fair trial would be infringed, where the competent national court finds in a case that a party is not in a position to comment effectively on evidence which pertains to a field of which the judges have no knowledge and which is likely to have a preponderant influence on the findings of fact.[173] The national court must in such case disregard such evidence that was obtained by way of a general and indiscriminate retention of traffic and location data found to be in violation of Art. 15(1) of the e-Privacy Directive read in light of Arts. 7, 8 and 11 and Art. 52(1) of the Charter.[174]

The CJEU cited to that effect its jurisprudence in *Steffensen*,[175] which in turn refers to the decision of the ECtHR in *Mantovanelli v. France*.[176] Both cases concerned technical issues before administrative courts, the former with regard to food safety, the latter with regard to liability in a case of medical maltreatment. The question arose as to whether the admission as evidence of results of expert analyses/reports on technical issues (quality of veal and pork sausages and respectively the excessive use of the anaesthetic Halothane), which went beyond the technical knowledge of the national court, entailed a risk of an infringement of the adversarial principle, given that in the *Steffensen* case the party was not given a right to request a second opinion in violation of EU law[177], while in *Mantovanelli* the party was entirely excluded from the preparation of the expert report.[178] Thus, although the administrative courts were not legally bound by the expert's findings, the technical analysis/report was likely to have a preponderant influence on the assessment of the facts by the courts.

The cited cases concern the situation in which the admission of evidence before a national court must be assessed against the right to a fair trial as laid down in Art. 6(1) ECHR, hence in principle similar to the one in the case at hand. Given the very specific technical questions involved in the cited cases and in particular the difference in the procedures involved (administrative/criminal), with the specificities and safeguards

necessary in the context of criminal proceedings, it is doubtful, however, whether the elaborations by the CJEU best capture and address the questions surrounding the use of unlawfully retained and/or accessed traffic and location data as evidence in criminal proceedings.

To that end, the ECtHR developed rich jurisprudence on Art. 6 ECHR. Generally, the ECtHR held that Art. 6 ECHR does not lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law.[179] It hence cannot determine whether particular types of evidence, such as evidence obtained unlawfully, may be admissible. The ECtHR stressed, however, that the proceedings as a whole, including the way in which the evidence was obtained, need to be fair.[180] It thereby looks at various aspects, such as the nature of the violation, whether the rights of the defence have been respected, the quality of the evidence, as well as the circumstances in which it was obtained and whether these circumstances raise doubt on reliability or accuracy of evidence, whether the evidence in question was or was not decisive for the outcome of the criminal proceedings, etc.[181] This test has been particularly also applied in cases concerning the question whether the use of information, which allegedly was obtained in violation of Art. 8 ECHR (right to respect for private and family life) as evidence rendered a trial as a whole unfair within the meaning of Art. 6 ECHR.[182]

In conclusion, it can be said that although national provisions on the admissibility and evaluation of unlawfully obtained information and evidence might differ across the EU, the jurisprudence of the CJEU and in particular also of the ECtHR on Art. 6 ECHR provides valuable guidance for national courts. Notwithstanding, it appears that a potential unlawfulness of a retention of or access to data used as evidence in criminal proceedings alone will hardly lead to an exclusion of that evidence from the criminal proceedings.[183]

IV. Considerations and Practical Implications for Data Retention Resulting from the Recent Jurisprudence

While it can be said that the CJEU in its recent judgements opened the door for a variety of possible exceptions to its established rule that a general and indiscriminate retention of traffic and location data is precluded, a legitimate question remains whether there is an actual possibility to walk through that door. While the openness from the CJEU might certainly be appreciated from the law enforcement perspective, if not so much from a privacy perspective, there are many practical, legal and technical aspects which need to be considered when trying to find solutions that can be applied in real life.

1. Safeguarding national security

To start with the most serious aim of safeguarding national security, the CJEU, as outlined above, allows for the preventive general and indiscriminate retention of traffic and location data. The criteria established in *Quadrature du Net* leave open a variety of questions. The CJEU requires to that end a serious threat to national security that proves to be genuine and present or foreseeable. All these requirements need to be defined in national law and the measure needs to be subject to judicial review.

Member States regularly establish a general risk assessment regarding their national security situation. While the retention, according to the CJEU, cannot be systematic in nature, the threat to national security, in effect and reality, could be of such nature. To defend their national interests and taking into account Art. 4(2) TEU, Member States may see the need to establish a consistently enduring high threat to their national security, which would justify the need for a generalised data retention scheme. It is likely that Member States and their national services are not going to have great difficulties to provide enough indications and evidence to establish such continuous state of being under serious threat. This is also comprehensible, as Member

States would want to be on the safe side and rather assess a risk as too high than as too low, with the then devastating consequences. Such a scheme would enable national security services to make use of the retained data in their effort to more effectively prevent and combat threats to national security, in particular terrorist attacks. The notion of a serious threat, which is "genuine and present or foreseeable" seems to offer sufficient leeway for Member States to establish their own assessment and to retain data on that basis.

What further supports this view is that the CJEU presumes that the existence of a threat to national security in itself establishes a connection between the data to be retained and the objective pursued – a requirement that the CJEU established in its earlier jurisprudence and considered indispensable. The CJEU, however, fails to provide any reasons for why such connection "must […] be considered", as it states in its judgement.[184] This means essentially that, in the CJEU's view, terrorist activities endangering or affecting the entire population form in themselves an objective criterion establishing a connection, between the data of the entire population and the objective of combating certain activities, such as terrorist crimes. This seems to be a too far-reaching assumption.

Moreover, there is a certain ambiguity left with regard to the term "safeguarding national security", which the CJEU sees as protecting essential functions of the State and the fundamental interests of society.[185] Although not congruent, the understanding of the term "fundamental State interests" under Article L. 811-3 of the French *Code de la sécurité intérieure*, subject of review by the CJEU in *Quadrature du Net*, is rather wide and includes apart from the prevention of terrorism, the protection and promotion of major foreign policy interests, economic, industrial and scientific interests or the prevention of organised crime. These and similar interests, such as the national employment situation or the national social and health systems, could well become the guiding principles in defining national security. It would not be the first time that restrictive or protectionist measures are justified with national security reasons. Against the background that according to the CJEU safeguarding national security encompasses the prevention and punishment of "activities capable of seriously destabilising the fundamental constitutional, political economic or social structures of a country", for which terrorist activities are mentioned by way of an example only, the scope of the data retention measure could in practice be interpreted a lot wider and used more frequently than initially envisaged or desired.

A key aspect for consideration by the Member States concerns the definition of a time limit and the possibility for a renewal of the instruction to the providers. How does this interact with the situation where there is a consistently high security threat in a Member State? Should national authorities in such situation request a fictitious shorter time period to comply with the CJEU's requirements and at the same time submit an advance request for renewal in order to avoid gaps in the retention, which would not only pose security but also legal risks?

Similarly, which competent national authority should request the instruction for renewal and which, if any, legal remedies are available to oppose such an instruction (and by whom – given that this measure would apply to everyone)? This might be left to the conditions and safeguards that need to be put in place, but the lack of clarity on these points and the level of uncertainty this leaves behind constitute serious challenges for all stakeholders involved.

Of crucial importance is the requirement that a court or an independent administrative body needs to verify that one of the situations justifying the general and indiscriminate retention actually exists and that the conditions and safeguards are observed.[186] Although this may reasonably be understood as a *prior* judicial review, the CJEU does not explicitly state so. Whether and under which conditions such judicial review may be carried out *ex post* and whether the court or independent administrative body will indeed be in a position to make such judicial assessment or whether it needs to rely to a large extent on the security assessment carried out and expert knowledge – hence be reduced to "rubberstamping" the request – remains to be seen.

https://doi.org/10.30709/eucrim-2021-020

Lastly, although this is not entirely clear from the judgement of the CJEU in the case *Quadrature du Net*, it is assumed that the data retained for the purpose of safeguarding national security may be used for any potential subsequent proceedings in a criminal investigation and prosecution, in particular in the situation in which a terrorist offence for which the data was retained could not be prevented and was actually committed. While the purpose of gathering intelligence information is to safeguard national security, *i.e.* to carry out preventive measures, the CJEU specifically mentioned prevention and punishment of the activities that threaten national security.[187]. Otherwise, from a purely practical angle, it would seem very unsatisfactory to be able to retain such data while not allowing the use of it in a subsequent criminal case before a national court. Linked to this question is however the scope of such retention in respect of crimes directly or indirectly linked to the e.g. terrorist crimes, such as money laundering. The focus of this problem could shift towards the question on admissibility and evaluation of evidence in criminal proceedings. Solely preventing a terrorist attack from happening on the basis of retained data and not consequently letting justice do its job, cannot be considered sufficient.

Overall, the CJEU opens a broad avenue for a general and indiscriminate retention of traffic and location data for the purpose of safeguarding national security. At the same time, it leaves open many questions that, as a whole, could seriously undermine the efforts made by the Member States to fulfil the requirements of the CJEU's jurisdiction, most notably the compliance with fundamental rights of the Charter.

2. Safeguarding public security (criminal offences)

In respect of the retention of traffic and location data for the purposes of combatting crime and safeguarding public security, the CJEU concluded that a general and indiscriminate, systematic and continuous data retention scheme is not justified, even for the fight against serious crime or prevention of serious threats to public security.[188] However, as outlined in the previous sections, the CJEU did allow for the "targeted retention" of traffic and location data, under certain requirements.

This follows the logic of the *Tele2* decision, and the CJEU elaborates in greater detail and provides additional examples in its recent judgments. Thus, the CJEU clarifies that a person subject of a targeted retention measure must generally have been identified beforehand as someone posing a threat to public or national security in a proceeding under national law.[189] This is a rather significant restriction, given that the purported aim and benefit of data retention is to actually identify such an individual from a large pool of persons on the basis of the data retained. This might also lead to difficulties because of another requirement set by the CJEU, i.e. the retention period. The CJEU requests retention periods that are limited in time and that data must be erased or anonymised at the lapse of the retention period. It is not far-fetched to believe that in many cases some, if not all relevant data, has been already erased by the time the targeted person has been identified and a request for retention made, leaving only the data retained from the immediate past available.

Moreover, the question remains on how to apply the restrictions with regard to "persons concerned" by a targeted retention in practice. As pointed out by the Belgian Constitutional Court in its reference, the difficulty lies in deciding whose data should be retained in a targeted manner, without being discriminatory. Such categorisation may also be incompatible with the presumption of innocence. In addition, it is also questionable whether a targeted retention of individuals is technically even possible since traffic data does not automatically allow for the categorization of individuals.[190] Such approach does also not offer solutions in relation to those with criminal intent, who can always find ways to circumvent chosen criteria, including by using prepaid cards for a short time, as well as first-time offenders that could not have been previously identified.[191] An additional challenge exists in cross-border situations, when persons concerned are frequently moving across borders, a tactic commonly used by organised crime groups, making a continuous targeting difficult if not impossible. It may also be that persons concerned are registered with several providers and for

service providers it is not easy to know exactly which particular person is making use of their services at a particular point in time. Service providers generally have information available about subscribers and contracts for their own billing purposes but defining which individual is making use of which particular service is a time-consuming and costly activity, if at all possible in view of the current and upcoming technological challenges, including the switch from 4G to 5G. Also, the possibility to retain data kept under enhanced end-to-end encryption methods by Over-The-Top content (OTT) services could ultimately render data inaccessible to law enforcement authorities. The switch to 5G in combination with the enhanced use of encryption methods may thus make it very difficult for service providers to retain (traffic and location) data of "persons concerned" in the context of a targeted retention scheme.[192]

As regards determining the geographical criterion by the national authorities, the CJEU seems to have "hot-spot" places in mind, with a high incidence of serious crime or that are particularly vulnerable to the commission of serious crimes, such as infrastructure, airports, stations or tollbooth areas. Although the avenue to apply a targeted approach in relation to specified geographical areas has been previously pointed to by the CJEU in *Tele2*, the questions on the practical applicability of such criterion remain persistent.

The retention of data related to a specific geographical area could equally easily be considered discriminatory and/or disproportionate. It could in practice entail that an extensive amount of data is retained from persons living, working or passing by the mentioned highly frequented areas without having any link to the objective pursued by the retention. Moreover, since the CJEU extended the use of the targeted retention *a fortiori* also to safeguarding national security, the geographical areas could (or should?) easily be extended preventively to areas targeted by terrorist attacks, such as large public places or areas housing governmental or state buildings.

In addition, the geographical criterion may not be consistent with the way service providers operate and it remains to be seen whether they can find technical and financially feasible ways of restricting the retention of data to specific areas. This very much depends on the location of the cell towers of each service provider. Furthermore, the signals put out by mobile telephones do not automatically correlate with predefined geographical limits and location data is not automatically included in the data collected by the service providers.[193]

Another consideration relates to the fact that certain types of crime, such as cybercrime, by nature cannot be restricted to specific geographical areas – they take place everywhere and from everywhere. Cyberspace is by definition not bound to geographical locations. But a restriction on the basis of a geographical location may also not be feasible for the more "general crimes." For example, many forms of organised crime cannot be restricted to specific geographic areas as a change in location is often part of the criminal strategy of organised crime groups.

An additional complication in this context concerns the different legal regimes service providers have to comply with, especially when they are operating at the EU or global level. Even if technical possibilities may be explored and created to ensure the retention of data related to specific individuals or specific geographical areas, such solution is likely to be burdensome and costly. Investments already made by service providers for accommodating and maintaining data storage centres may not be sufficient for a targeted retention approach. Technical expertise to maintain and keep up to date these systems is needed[194] and service providers have to mitigate data breaches and cybersecurity risks. Reimbursement schemes by governments to cover for such costs vary greatly (and generally do not involve the investment costs that need to be made at the beginning) and it could therefore be the case that ultimately consumers will have to carry those costs themselves.

Furthermore, as regards the retention period, beyond the still unanswered question about the appropriate – or proportionate – length of such period, the CJEU allows the possibility for extensions, similarly to the case of safeguarding national security. All these extension decisions in themselves would impinge on the fundamental rights of the persons concerned. Nonetheless, unlike in the case of protecting national security, the CJEU does not explicitly mention any requirement for a judicial review of such decisions here. These decisions are also separate from a request for access to such retained data, however, given their intrusive nature, effective judicial review seems indispensable in the context of the CJEU's approach of targeted retention.

Generally, the possibility of a targeted retention scheme is connected to the concept of serious crime. Art. 1(1) of the invalidated Directive 2006/24, which concerned the subject matter and scope, left the definition of "serious crime" to each Member States' national law.[195] While the CJEU established in *Tele2* that serious interferences can only be justified by the fight against serious crimes, it failed two years later to reply to the question of the referring *Tarragona* court in its decision *Ministerio Fiscal* what exactly determines the seriousness of the offence.[196] Although in its recent jurisprudence, the CJEU at least concedes that child pornography offences as defined in Art. 2(c) of Directive 2011/93[197] constitute serious offences,[198] it generally evades answering this question in full. As the harmonisation of the definition of serious crime seems, as it currently stands, is not possible at the Union level, given the lack of harmonisation of substantive criminal law and the specificities of each national judicial system, an incoherent application of the concept of "serious crimes" inevitably leads to divergences in the interpretation and application of the CJEU's jurisprudence, as well as in the use of data retention rules across the Union and eventually in the level of protection of fundamental rights. Even if the list of serious crimes within Member States were to be identical, it could still lead to discrepancies between Member States and a potential unequal treatment of suspects and accused persons, in particular in cross-border situations. It may also lead to unwelcome situations where certain crimes, which are considered to be minor, e.g. online fraud, are part of a bigger scheme of serious crimes, which could not have been uncovered without the retention of this data. Moreover, there are also crimes that may not be considered "serious", such as cyber-grooming or stalking, where the retained data remains the only information available to identify a suspect and bring the crime to justice.

In sum: same as in the case of safeguarding national security, the CJEU reinforces its jurisprudence in favour of a well-designed "targeted retention" of traffic and location data for the purpose of safeguarding public security, however, it leaves many questions open and does not sufficiently outline how such design could work in practice. Data retention for the purpose of fighting (serious) crimes remains therefore challenging for the Member States, bearing the risk of failing to comply with the CJEU's jurisdiction and fundamental rights of the Charter.

3. Retaining IP addresses and civil identity

Concerning the retention of IP addresses, the CJEU has taken into account considerations put forward by a number of Member States and acknowledges that, where an offence is committed online, the IP address may be the only means of investigation to identify the person to whom that address was assigned at the time the offence was committed.[199] This outcome resembles the findings of the Constitutional Court of Portugal in the case cited above (II.3). Nonetheless, for all the operational reasons that might speak in favour of the retention of IP addresses, the purpose driven approach followed by the CJEU is somehow unsatisfactory, given the significant impact of this exception.

Generally, the CJEU neither proffers convincing legal arguments for the conclusion reached, nor is the required connection between the data retained and the objective pursued, as required under the CJEU's case law, visible neither at first nor at second sight. It is also astonishing that the CJEU builds its argument around

the circumstance that IP addresses would otherwise be unavailable as they are not retained by the providers of electronic communication services.[200] In fact, the non-retention results from the very fact that internet users enjoy the same protection of their fundamental rights under Arts. 7 and 8 of the Charter also in relation to IP addresses.

The CJEU also does not draw any distinction between static and dynamic IP addresses. While the desired goal – the identification of the user – is the same, the legal and practical handling of static and respectively dynamic IP addresses differ. From a technical point of view, dynamic IP addresses are more difficult to obtain for law enforcement authorities as more data is needed from service providers to identify the user behind a connection. Since identifying the users behind dynamic IP addresses generally requires the use of other data, it is hence unclear whether they fall under the CJEU's ruling related to the generalised retention possibility for IP addresses assigned to the source of a connection. Thus, the CJEU misses an opportunity to elaborate in greater detail on justifying this exception and the related questions, and whether this measure is indeed suitable and effective in pursuing the desired objective, *i.e.* to identify the end user.

Furthermore, the IP address itself may not be sufficient and other identification data needed to identify a relevant user in an investigation, for example the connection port, the date and time of the connection and its duration as well as the Media Access Control (MAC) address and the International Mobile Equipment Identity (IMEI) code. This information is often difficult to obtain when the Network Address Translation (NAT) technology is used. IP addresses, especially dynamic IP addresses, are often assigned to more than one end-user because of the wide use of NAT technology. NAT is used to thwart the limited availability of IPv4-addresses to make connections. Using NAT, there could be thousands of users linked to one single public IP address, making it virtually impossible to identify the user who is of interest in a criminal investigation. And even if only a relatively small number of potential subscribers are identified as potentially relevant to the case, this will mean that investigative powers will have to be used against innocent citizens in order to identify the single user of interest. This infringement of fundamental rights could be mitigated or even avoided if the system was such that only the relevant subscriber could be identified. In addition, it is even more difficult to identify the relevant user when persons are using the internet or other digital services in public spaces such as internet cafés.

The issues linked to the NAT technology and dynamic IP addresses are not new. Although the more advanced IPv6, which makes available an immeasurable amount of IP addresses for use and thus makes the use of the NAT technology obsolete, became available in 1999, technical problems still persist. In fact, to date, the IPv4 and IPv6 systems exist in parallel.[201] According to the Google statistics consulted in September 2021 the availability of IPv6 connectivity in the EU ranges from 2% in Spain to 52% in Germany[202]. It can be expected that this situation is still going to remain at least in the short to medium term. For service providers it remains very complex and costly to retain the information necessary to identify users via dynamic IP addresses and they hence do not see the need to retain them except they are under legal obligation.

Another complication that should be kept in mind is that those with criminal intent could make use of modern software to anonymise and hide their IP addresses. In addition, the question also arises what is considered to be a reasonable time for retaining IP addresses.

As regards the data relating to the civil identity of users of electronic communications systems, the CJEU considers the retention of this data category to be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general and safeguarding public security, without imposing any limitations as regards the retention period. While the CJEU seems to try its best to offer more openings to the current difficulties for law enforcement authorities, the exact scope of this part of the ruling is not entirely clear. In particular, it is unclear whether the civil identity data category concerns the same type of

data as the subscriber data category, in line with the definition used in the e-evidence package[203] and the Budapest Convention[204]. In order to better understand the practical implications of this concept, it would be useful to know from the CJEU which data can be retained in relation to the civil identity of a user. Moreover, given that even a non-serious interference with fundamental rights still remains an interference that needs to comply with the requirements of Art. 52(1) of the Charter, it would have been desirable, if the CJEU had elaborated in greater detail on the reasons which led to its conclusions, when it sought to strike a balance between the rights and interests at issue.

4. Expedited retention or 'quick freeze'

As regards the possibilities of expedited retention, the CJEU acknowledges the situation that traffic and location data should be retained after the normal time periods for commercial processing and storage by the service providers have elapsed. This is the case where the data could be necessary to shed light on serious criminal offences or acts adversely affecting national security. The CJEU highlights that this could be in situations where the adverse effects on national security have already been established and where, after an objective examination of all circumstances, the adverse effects may reasonably be suspected.[205] The CJEU mentions that this measure can only be applied with regard to traffic and location data, that the duration must be limited to what is strictly necessary (with an extension possible), and that the instruction decision vis-à-vis the service providers should be subject to effective judicial review.[206] An extension of the retention possibilities to other persons is allowed, provided this is done on the basis of objective and non-discriminatory factors. Separate conditions are set out for the access to the data that was retained in this context.

In the absence of broader possibilities to retain data, the preservation of data related to a specific offence or a specific suspect was discussed as an alternative solution for law enforcement authorities. In Member States, this measure is usually referred to as the "quick freeze". If one can assume that the CJEU refers to the same notion, this measure refers to the request from law enforcement authorities or the prosecution service to preserve specific existing or past data stored by service providers for other purposes. However, as underlined by several law enforcement authorities, expedited retention is not really a suitable alternative to a generalised data retention scheme.[207] "Quick-freeze" merely saves available data from being erased, while the retrograde data that law enforcement authorities are most interested in cannot be retrieved *ex post*.[208] Moreover, the mechanism of a quick freeze can only apply from the moment there is a suspicion of a crime. This makes it necessary that at least a level of suspicion is established and a specific person is identified as suspect and at that point in time, there is still relevant data to be frozen. Furthermore, the success of the measure very much depends on the national legal framework in place and if, and what types of data are (mandatorily or voluntarily) kept for which time period by service providers. Even if the national legislation allows for the preventive and mandatory retention of data by service providers in order to later on be able to request for a quick freeze, the reality is that, in comparison to a generalised data retention scheme, not all types of data can be kept in the same manner and for the same period of time.[209] Again, the same question of what duration could be defined as strictly necessary leaves room for interpretation as well as the question at what point in time an extension of the measure should be requested.

Another practical difficulty for law enforcement and judicial authorities that may arise relates to the fact that access to preserved data obtained for the purpose of tackling serious crime or protecting national security is not allowed for prosecuting or punishing "an ordinary criminal offence". A similar discussion could be held here as was done regarding the notion of "serious crime" (see above 2.). What should be understood under these concepts, is left to Member States, hence the interpretation and application may vary. But what happens if an ordinary criminal offence is inextricably linked to the serious crime or national security situation for which access to the data was granted? Does this imply that the offences need to be investig-

ated and/or prosecuted separately? Or, could this situation be left to be reconciled through national rules on the admissibility and evaluation of evidence?

Moreover, the CJEU widens the scope of this measure by stating that the data requested through a "quick freeze" need not be limited to the persons specifically suspected of the crimes or act in question but also to other persons or geographic areas. The question is how objective and non-discriminatory factors can be formulated in order to avoid that the data of random bystanders is retained, thereby seriously interfering with the privacy of a potentially large group of people. After all, it is relatively easy to argue that any data can "shed a light" – as the CJEU puts it – on offences or acts authorities became aware of. Furthermore, as previously mentioned, the exception of an expedited retention may be used in conjunction with other exceptions justified under Art. 15(1) of Directive 2002/58, which could lead to the situation that more data of a variety of persons is retained for different purposes and could be used in a combined manner.

5. Automated analysis and real-time collection

As regards the particularly invasive intelligence techniques of an automated analysis and real-time collection of traffic and location data, the CJEU, to a large extent, adopts the same requirements established in the context of measures for the purpose of safeguarding national security. Accordingly, all the points raised under III.2.c) aa) above are valid here too. This concerns in particular the scope of the term "national security", the possibility for an enduring threat, the assumption (or rather the absence) of the existence of a link between all those whose data will be analysed (i.e. all persons using electronic communication systems!) and the threat, the scope and effectiveness of judicial review, and the handling of linked offences identified. Also, the terms and conditions applied by the CJEU – "valid reason to suspect" an involvement "in one way or another in terrorist activities" – seem to offer wide room for interpretation despite the very intrusive quality of the measure in question.

Moreover, given the specific nature of this measure, which applies parameters based on pre-established models and criteria, additional questions arise. The CJEU clarified that these models and criteria have to be determined in a non-discriminatory manner. But in a similar way as in the case of "targeted retention" (above III.2.c) bb)), this requirement imposed by the CJEU might turn out to be difficult to apply in practice. The use of pre-defined and set parameters might lead to a lack of traceability and comprehension of the output. For this reason, it might also be difficult to define the subject of judicial review. Moreover, such systems often bear the risk of generating a (at times significant[210]) number of wrong hits and errors and generally have an inherent deficiency with respect to transparency and control. It is doubtful that a manual review alone would be able to address such errors and deficiencies. In addition, a manual review of an automatic decision-taking system may also bear the risk of merely legitimising the automated decisions taken, without actually making the necessary comprehensive assessment due to the potential volume and the time constraints.[211] In the end, it remains entirely unclear, who should control and review such systems that are run by private service providers, on which basis and how often.

V. Data retention in the context of the negotiations on the e-Privacy Regulation

On 10 January 2017, the Commission put forward a proposal for a e-Privacy Regulation[212] to update the current rules to technical developments, to adapt them to the GDPR and to repeal the "e-Privacy Directive" from 2002. The objective of the e-Privacy Regulation, which, unlike the Directive, would apply directly across the Union, is to reinforce trust and security in the Digital Single Market, in particular strengthening security and confidentiality of communications and establishing clearer rules on tracking technologies, including cookies

as well as on spam.[213] The e-Privacy Directive was considered not to keep pace with the technical developments leaving a void of protection of communications conveyed through new services. The Commission proposal did not explicitly make any specific provision on data retention. It merely echoed in its Art. 11 the substance of Art. 15 of the current e-Privacy Directive. However, the draft Regulation aligns the scope of Art. 11 with Art. 23(1) GDPR, thus in effect, widens it considerably by introducing a general clause of "other important objectives of general public interest of the Union or of a Member State" to the list of objectives for which the rights enshrined in the draft Regulation may be restricted. Member States may hence keep or create national data retention regimes that provide, *inter alia*, for targeted retention measures, in so far as such regimes comply with Union law, taking account of the CJEU's jurisprudence on the interpretation of the e-Privacy Directive and the Charter.[214]

The European Parliament (EP) adopted its report on the draft proposal in the same year.[215] With regard to Art. 11 of the draft Regulation, the EP seeks to strengthen the safeguards, notification and transparency requirements as envisaged in the GDPR; however, the EP supports a narrower and more precise list of objectives provided in Art. 11 of the proposed Regulation, which may justify a restriction of the rights. It hence supports deletion of the general clause of "other important objectives" from that list.

The Council took more than four years to adopt its negotiation mandate under the Portuguese Council Presidency on 10 February 2021.[216] The question on data retention has been a highly debated issue discussed during the negotiations in the Council, in particular following the latest judgements of the CJEU.[217] Art. 2(2) of the General Approach of the Council provides for the material scope of the Regulation and stipulates that it shall not apply to "*(a) activities falling outside of the scope of Union law and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities, whether it is a public authority or a private operator acting at the request of a public authority*". According to the Council's General Approach, the Regulation's material scope shall also not apply to "*(b) activities, including data processing activities, of competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".

In particular, the exclusion of retaining data for national security purposes from the scope of the proposed Regulation, as listed in Art. 2(2)(a) of the Council's General Approach, seems to be a response to the case law of the CJEU in relation to Arts. 1(3) and 15(1) of the e-Privacy Directive. This echoes the findings of the CJEU in the recent cases, where the CJEU differentiated between the old and repealed data protection Directive 95/46 and the e-Privacy Directive (see details above under III.2.a). Following its General Approach, the Council text would swipe away the jurisprudence of the CJEU at least as far as it concerns national security and defense. This would also, in a way, reinstate the situation as under Directive 95/46, which was overcome by the GDPR. In consequence and as intended, measures such as the retention of data in the context of safeguarding national security and defense would fall within the sole responsibility of national law and the ECHR. Nonetheless, given the role of the CJEU as the guardian of the Charter, it could be that the CJEU would review the principles it had established with regard to the protection of the fundamental rights under Arts. 7, 8 and 11 of the Charter directly, given the CJEU's broad understanding of "implementing Union law" within the meaning of Art. 51(1) of the Charter.[218] This means that even if the e-Privacy Regulation were to entirely exclude the retention of traffic and location data from its scope or for safeguarding national security and defense only, and instead this would be governed solely in national law, the CJEU could review the compliance of such national provisions with Arts. 7, 8 and 11 of the Charter in any case.

In respect of the fight against crime and the protection of public security, Art. 6(1)(d) of the Council text permits service providers to process electronic communications data where it is necessary to comply with Union or national rules to safeguard the prevention, investigation, detection or prosecution of criminal

offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security. Art. 7(4) of the Council text acts as the general rule on data retention and allows Union or national law to retain electronic communications metadata for a limited period of time in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security under the condition that the essence of the fundamental rights and freedoms is respected and it is a necessary and proportionate measure in a democratic society. In comparison with the jurisprudence of the CJEU, the Council's General Approach leaves out the distinction between the notions of serious crime and criminal offences in general as well as the conditions linked to the retention thereof. Moreover, the General Approach does not make any distinction for data categories.

The Council's General Approach received fierce criticism *e.g.* by the German data protection authority, which generally sees in it a "harsh blow to data protection", while expressing serious concerns with regard to the revisions made on data retention.[219] Finding a common ground on the e-Privacy Regulation has been challenging in the course of the last four years. The trilogue negotiations started on 20 May 2021 and it is difficult to predict what the outcome of these negotiations will be. There is a clear need to update the 20-year-old e-Privacy Directive with a modernised piece of legislation. Going back in time to the level of Directive 95/46 for the purpose of excluding retention measures to safeguard national security from the scope of the new e-Privacy Regulation seems not to be a viable way. Moreover, as seen, the desired result – taking data retention for the purpose of safeguarding national security out from the scope of the proposed Regulation and the review by the CJEU – could in the end turn out to be wishful thinking. Despite all the misgivings expressed by the Parliament against and, by contrast, the strong wish expressed by the Council for a data retention regime, a set of recalibrated rules on data retention following the lines and limits set by the CJEU might be a prudent and yet feasible way forward for the e-Privacy Regulation after all.

VI. Conclusions

Data retention is not off the table. It never was. However, the discussions surpass the more radical (and at times emotionally charged) discussions *pro et contra* data retention as such and, thanks to the CJEU, now take a far more differentiated and diligent shape. The CJEU shed light on and recalibrated in detail the various facets of this wide, complex, and sensitive field of law, politics and life. It sought to establish a balance between the various entangled fundamental rights and freedoms. This debate that is often being portrayed as a "clash" between those who seek to defend liberty and those who seek more security will continue. And that's good. Each society and generation have its own expectations and faces its own challenges, while, with the changes that emerging (not least digital) technologies bring about, the questions surrounding the two notions of liberty and security remain to be asked and will need to be answered now as well as in the future. That is what the CJEU does in the EU's area of freedom, security and justice and this is what the CJEU needs to do.

The CJEU is also not legislating, as it is sometimes said. The CJEU, in the cases brought before it, sets the limits it sees as being necessary in order for legislation to comply with the principle of proportionality and the EU Charter of Fundamental Rights. That is what the legislator has to respect if it wishes to regulate the retention of data for the purpose of preventing serious threats to national security and combating crimes. The limits apply to both, the EU legislator in the event that this matter is regulated at EU level or, in the absence of EU action, the national legislator, who is bound by the principles and safeguards enshrined in the Treaties. Notwithstanding, data retention raises a number of questions.

From the outset, firstly, the legislator would need to proffer convincing evidence why it chooses to impose obligations on private providers of electronic communication services to retain different types of data in

https://doi.org/10.30709/eucrim-2021-020

order to allow access to competent national authorities. Is the retention of data capable of bringing the desired added value in the prevention of serious threats to security and combating crimes? This question has been consistently flagged in the past, but has not been convincingly answered to date. It is a legitimate question, given the inherent serious interference with and violations of fundamental rights of a potentially very large number of persons (if not the entire European population), who might be entirely unrelated to the pursued objectives – something that could be depicted as a "mass incrimination".

The scarce number of studies that attempt to shed light on this question, all struggle with the lack of reliable information. The very illustrative and extensive study prepared by the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, dates back to 2011 but still provides valuable insight and anecdotal evidence in this matter.[220] It particularly highlighted the lack of reliable statistical data and systematic empirical studies as well as the rather diverging views of the practitioners consulted.[221] Although the experience from anecdotal evidence provided in the study might be considered as exemplary, such evidence cannot be considered empirically deduced or proven. The Max Planck study outlined that, overall, there are no reliable indications that the retention of traffic and location data had an impact on the conviction rates. It particularly also did not find any indication that retained traffic or location data had any impact on the prevention of terrorist activities, while there are reasons to believe that such data might contribute to the investigations in the aftermath of terrorist acts. Against the background of the lack of relevant and/or reliable data, the study stressed that it is not excluded that traffic and location data could provide indications to initiate investigations and support complex investigations.[222] But even if such anecdotal evidence could indeed be established, such evidence alone would have no significant impact on the overall picture. However, for want of relevant and reliable data, it is difficult to use the study in favour or against data retention.

The study[223] prepared by the Legal Service of the European Parliament also deplores the lack of data and stressed particularly that it is not possible to establish a direct correlation between the existence of data retention laws and crime statistics. The study indicated that too many parameters need to be considered in order to be able to evaluate the reason for statistical changes.[224] The same problem is outlined in the most recent study on this matter, commissioned by the European Commission.[225] This study, which looked into the legal framework and practices of ten Member States, yet highlighted that the information cannot be seen as representative of the stakeholders' view due to the limited information on this issue.[226]

The CJEU does not seem to question the added value of a data retention regime, when it stated in its decision *Digital Rights* that the eventually invalidated Data Retention Directive may be considered appropriate for attaining the objective pursued, without providing any reasons how it reaches such conclusion. Indeed, the question whether a measure is suitable or appropriate to attain the desired purpose may be posed several times when reading the recent judgements of the CJEU on data retention. When examining the measures, the CJEU seems to simply want to assume that this is the case – i.e. that the measure is indeed appropriate. This approach gives a blemish to the various exceptions justifying an interference with the fundamental rights of the European citizens, as put forward by the CJEU. But beyond that, from a more political point of view, the legitimacy of such invasive measures could be considerably increased, if the European and/or national legislator were to provide substantiated and convincing evidence of the added value of a data retention regime. This would also help in overcoming any polarising and simplistic debates on this important matter.

Secondly, in the decisions on data retention, the CJEU very much acts like a constitutional court. This is yet another *facette* of the CJEU, in addition to the broad variety of matters it has competence over (most recently, also in criminal proceedings of the European Public Prosecutor's Office[227]). The CJEU had to deal with the protection of fundamental rights in the past, prior the enactment of the Charter on Fundamental Rights. Already in 1969, the CJEU established in the *Stauder* case that fundamental rights are part of the gen-

eral principles of Community law and that they are protected by the CJEU.[228] Nonetheless, thorough reflection should be spent on the question whether the existing structure of the CJEU and the legal and procedural framework is indeed best suited for the CJEU to carry out multiple functions as "one court for everything" and grant and ensure the necessary effective legal and judicial protection of fundamental rights in the EU.

Linked to the protection of fundamental rights, questions arise in respect of the lack of coherence between the jurisprudence of the Luxembourg court and the Strasbourg court. Although the CJEU reiterated in its recent decisions on data retention that pursuant to Art. 52(3) of the Charter, the corresponding rights of the ECHR form only the minimum threshold of protection, a divergent jurisprudence might lead to serious uncertainty with regard to the level of protection of human and fundamental rights in Europe, in particular also as the CJEU in its findings stresses that the fundamental rights in the Charter correspond to the rights under the ECHR. Such lack of coherence could potentially lead to situations, in which Member States face conflicting obligations to be followed under the principle of primacy of EU law on the one hand and obligations under the ECHR on the other. Although such concern might be considered theoretical only, the present lack of coherence could undermine the existing complex multi-layered relationship between the CJEU, the ECtHR and national constitutional courts. Moreover, while Art. 53 ECHR leaves room for a higher protection of human rights at national level, as long as the minimum standards guaranteed under the ECHR are complied with, a higher level of protection under national constitutional law might run into conflict with the principle of primacy of EU law, if various different national standards exceeding those guaranteed under the Charter were to be applied.[229]

Another aspect concerns the review of the fundamental rights by the CJEU. The CJEU identifies a number of fundamental rights in the Charter – Art. 7 (respect for private and family life), Art. 8 (protection of personal data), and Art. 11 (freedom of expression and information) – and balances these rights and interests against those which follow from Art. 3 (right to the integrity of the person), Art. 4 (prohibition of torture and inhumane or degrading treatment of punishment), and Art. 6 (right to liberty and security). Thereby, the CJEU did not reach a very deep level of examination. It is striking that the CJEU did not even consider the legitimate rights and interests of the private service providers as enshrined in Art. 16 (freedom to conduct a business) of the Charter. In view of the various possible obligations that may be imposed on the service providers in line with the jurisprudence of the CJEU, which has a considerable impact on business decisions, and which entails significant costs (investment and running costs) it is remarkable that the CJEU, as the guardian of the Charter, remains entirely silent on this point, irrespective of the fact that in some cases these costs may be (fully or partly) reimbursed. Art. 16 of the Charter might deserve attention also from another perspective, touching the question of legal standing, namely whether, how and to which extent private entities, such as private service and network providers, may in themselves invoke the violation of Arts. 7 and 8 of the Charter in the context of the retention of traffic and location data of their users or subscribers, *i.e.* third parties, or at least "trigger" an incidental review of violations of these fundamental rights of their users and subscribers. Although legal persons may invoke the rights enshrined in Arts. 7 and 8 of the Charter[230], the CJEU has reviewed the compliance of national data retention regimes with the Charter and potential violations of Arts. 7 and 8 of the Charter in relation to users and subscribers only and not the service and network providers, while Art. 16 of the Charter has never been a subject of discussion in that context. In general, it would be desirable if the CJEU developed a more elaborate approach in reviewing potential interferences and violations of fundamental rights in the EU.

Thirdly, while the CJEU cracked the door open to various exceptions justifying the retention of traffic and location and other data, it remains unclear whether Member States, in practice, may indeed safely walk through that door. Even if the CJEU recalibrated its jurisprudence on data retention and is expected to continue doing so in the future,[231] there are still many questions left open, which, if unanswered, will continue to hinder the efforts made by the Member States to establish a balanced and Charter-compliant data reten-

tion regime. Moreover, experience from the past has demonstrated that the judgements of the CJEU did not always lead to the desired common understanding on how to design a meaningful and functioning data retention regime that complies with the *acquis* and the Charter, nor has the recent jurisprudence of the CJEU, as seen in the different approaches taken after the *Quadrature du Net* judgement by the referring courts.[232]

The CJEU could and should have taken the opportunity to shed more light on the various legal questions, with regard to the terms and requirements it established on data retention and should also have taken to a greater extent a careful look at the practical feasibility of the solutions it suggests. It may be that this is left for future judgements the CJEU is going to render. However, given the importance of the matter and the significance for the protection of fundamental rights in the Union on the one hand and maintaining security on the other, this seems like a missed opportunity.

In his Opinion[233] delivered on 18 November 2021 on the pending cases C-793/19 *SpaceNet* and C- 794/19 *Telekom Deutschland*, case C-140/20 *Commissioner of the Garda Siochana and Others* and joined cases C-339/20 *VD* and C-397/20 *SR*, Advocate General (AG) *Campos Sánchez-Bordona* hints to some of the concerns raised in this article. These include the boundaries for the invocation of national security to allow a general and indiscriminate retention of traffic and location data,[234] potential uncertainties with regard to the scope of state security,[235] the difficulties in developing criteria for an effective and non-discriminatory targeted retention,[236] and the distinction between static and dynamic IP addresses and the impact of the Ipv6 protocol.[237] However, the AG does not elaborate in greater detail on them. Overall, he restates the line, which the CJEU has taken in its judgments in *Quadrature du Net* and *Prokuratuur,* and remains silent on the various pertinent question that follow from that jurisprudence.

The protection of personal data is without doubt one of the Union's success stories. The Union sets and promotes very high standards, and its data protection *acquis* has become a "gold standard" that is referred to as a model also for other countries in the world. At the same time, the Union is a "Union that Protects" and there are several measures to be put in place under the Union's Security Agenda. In its various judgements on data retention over the past years, the CJEU never entirely closed the door to the possibility of retaining data for the purpose of safeguarding national security and fighting serious crimes. All discussion on this topic is therefore guided by the importance of providing effective tools to fight crime, on the one hand, and the need to respect fundamental rights, in particular the rights to privacy, protection of personal data, non-discrimination and presumption of innocence, on the other hand.

Undoubtedly protecting private data is of utmost importance. However, the rights and interests following from the e-Privacy Directive and Arts. 7, 8 and 11 of the Charter do not mean that those rights and interests prevail over all other interests. Personal data is generated and used in all our daily lives. Nonetheless, the protection of personal data needs to be balanced in a sound and sober manner with other objectives and against the legitimate rights and interests of others; it obviously cannot trump all other rights and interests. The protection of data must also not become an impediment to the dynamic process of digital development. This applies equally to the positive aspects of new technologies as well as to their negative ones (use to commit crimes). Eventually, it is also about the question which price we want to pay to live in a free and secure society and how much criminality our society is capable of accepting for the benefit of safeguarding fundamental rights and freedoms.

The ongoing negotiations on the e-Privacy Regulation could tackle some of the open questions and address practical impediments, as long as this will be a step forward (and not backwards in the form of limiting the scope). However, it is not possible to predict the outcome and the speed of the negotiations yet.

In view of the persisting uncertainty on this topic and in view of the recent jurisprudence of the CJEU on data retention, it seems clear that there is a compelling need for finding a common ground. Such common ground

could be established by way of a legislative approach at least on a set of definitions and basic notions at the Union level. This approach could provide the desired added value and the necessary legal certainty, also given the increasing number of cross-border investigations and prosecutions in the EU and the fact that service providers are established all over Europe (and the rest of the globe). Definitions on the categories of data should be aligned as much as possible with the existing *acquis* and future instruments, e.g., the future legislation on the EU-internal e-evidence package. A legislative approach at Union level could also include the newly established notion of civil identity data. Although more difficult, EU legislation could also include specific time limits under which data may be retained, depending on the sensitivity of the data in question and the purpose for which it is retained. From a fundamental rights point of view, it could also be useful to define in which situations a prior judicial authorisation is required and how to handle urgent cases. Another legislative aspect could concern a transparency mechanism which would provide an overview on the use and frequency of the measures across the Union. Even if on a small scale, such common legislative approach could put data retention on a more solid ground than the highly useful but more request-driven and hence piecemeal approach provided by the CJEU through its jurisprudence.

In conclusion, the recent jurisprudence of the CJEU does not bring about the necessary clarity to mark an end to the discussions as to whether data retention is a suitable tool that provides added value in the prevention and investigation of crimes and the protection of national security in the EU. For this it leaves too many questions open, in particular on how to implement the requirements of the CJEU jurisprudence in practice. At the same time, following years of controversy and numerous judicial decisions at national, Union, and European level, one can hardly speak of a beginning of data retention in the EU; nonetheless, the recent jurisprudence of the CJEU at least opens up many new avenues for consideration and reflection. These new avenues could be taken up and possibly channelled to a new legislative proposal with a limited scope at Union level.

Even so, without clear and convincing reasons supporting the suitability and added value of data retention for the purpose of preventing and fighting crimes and safeguarding national security, any legislative measures discussed will always be marred with a stain. But the CJEU will soon have another opportunity to shed more light on this matter.[238]

---

1. Cf. the broad support expressed by Ministers at the March 2021 Justice and Home Affairs Council for a functioning data retention regime. The Portuguese Presidency stressed on that occasion: *"The retention of data is a crucial tool for our law enforcement authorities when carrying out investigations, and it is clear the current situation of uncertainty increases the risks to the security of our citizens. Today we reiterated our commitment to finding a common solution; one which allows our police and judicial authorities to carry out their work while fully ensuring the rights to privacy of our citizens."* See: Informal video conference of justice ministers - Consilium (europa.eu).↩
2. E.g. Germany's former Minister of Justice, Sabine Leutheusser-Schnarrenberger, „Goodbye Vorratsdatenspeicherung", *Verfassungsblog*, 8 October 2020, <https://verfassungsblog.de/author/sabine-leutheusser-schnarrenberger/>, accessed 9 August 2021.↩
3. Charter of Fundamental Rights of the European Union (hereinafter "Charter"), *O.J.* C 326, 26.10.2012, 391.↩
4. Cf. e.g. decision of the Constitutional Court of Romania, Decision no. 1258 of 8 October 2009, Official Gazette no. 798 of 23 November 2009, or decision of the Bundesverfassungsgericht (Federal Constitutional Court of Germany) of 2 March 2010, 1 BvR 256/08, both decisions rendered before the CJEU took a stance on the matter in its judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger a.o.*. The jurisprudence of the CJEU was taken into account by subsequent decisions in several Member States, such as Austria, the Netherlands, Slovakia, and Slovenia.↩
5. Cf. ECtHR, 25 May 2021, *Big Brother Watch and Others v. the United Kingdom* (applications nos. 58170/13, 62322/14 and 24960/15); ECtHR, 25 May 2021, *Centrum för rättvisa v. Sweden* (application no 35252/08); ECtHR, 2 December 2008, *K.U. v Finland* (application no. 2872/02).↩
6. Conclusions of the European Council meeting of 10 and 11 December 2020, EUCO 22/20, point 26, <https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf>, accessed 9 August 2021.↩
7. Cf. the informal video conference of justice ministers - Consilium (europa.eu).↩
8. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *O.J.* L 105, 13.4.2006, 54–63.↩
9. Judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger a.o.*↩
10. Ibid, para 49.↩
11. Ibid, para 57.↩
12. Ibid. para 60.↩

13. Ibid. para 63.↩
14. Ibid. para 66.↩
15. Ibid. para 68.↩
16. Such as in Austria, Belgium, Slovakia, and the Netherlands.↩
17. The purpose of the data retention directive was to combat serious crime, not all types of crime – cf. Art. 1(1) of Directive 2006/24, *op. cit.* (n. 8).↩
18. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter "e-Privacy Directive"), *O.J.* L 201, 31.7.2002, 37–47.↩
19. Judgement of 21 December 2016, Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB/Watson*, para 59.↩
20. Cf. n. 19.↩
21. Ibid, para 85.↩
22. Art. 15(1) of the e-Privacy Directive – headed 'Application of certain provisions of Directive [95/46]' – reads as follows: "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive [95/46]. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."↩
23. CJEU, *Tele2/Watson, op. cit.* (n. 19), para 89.↩
24. Ibid, para 90.↩
25. In *Digital Rights*, the CJEU did not see a need to examine the validity of Directive 2006/24 in the light of Art. 11 of the Charter, given the violation of Arts. 7 and 8 of the Charter, cf. CJEU, *Digital Rights Ireland and Seitlinger a.o.*, *op. cit.* (n. 9), para 70.↩
26. CJEU, *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 94.↩
27. Ibid, para 98, 99.↩
28. Ibid, para 100.↩
29. Ibid, para 102.↩
30. Otherwise, as the Court stressed, the national legislation in question would affect the essence of those fundamental rights, ibid, para 101.↩
31. Ibid, para 101.↩
32. Ibid, para 107.↩
33. Ibid, para 104, 105.↩
34. Ibid, para 108-111.↩
35. Ibid, para 115.↩
36. Ibid.↩
37. Ibid, para 116.↩
38. Ibid, para 117.↩
39. Ibid.↩
40. Ibid, para 119.↩
41. Ibid, para 120, 123.↩
42. Ibid, para 121.↩
43. Ibid, para 122.↩
44. Ibid, para 65-81.↩
45. Ibid.↩
46. Ibid, para 72, 73.↩
47. Ibid.↩
48. Ibid, para 75-78. Cf. also Advocate General Saugmandsgaard Øe's opinion of 3 May 2018 in the Case C-207/16 *Ministerio Fiscal*, para 47, where he makes a difference between data processed directly in the context of state activity of a sovereign nature and data processed as an activity of a commercial nature and made available to authorities subsequently.↩
49. Judgement of the Constitutional Court of Portugal of 13 July 2017, no. 420/2017. The judgement concerned a case of child abuse, where a request by a prosecutor for authorisation to transmit data to identify a user to whom an IP address had been assigned was rejected by the District Court of Lisbon in October 2016 on the grounds that the Portuguese Law 32/2008, which transposed Directive 2006/24/EC, was unconstitutional in view of the CJEU's *Digital Rights* decision. The Constitutional Court concluded that Portugal, when transposing the Data Retention Directive, introduced an extensive and complex framework, including on access to and protection of retained data, and that these differences ought to be taken into account. The Constitutional Court hence declared the retention of subscriber information with respect to dynamic IP addresses on the basis of the Portuguese Law as constitutional.↩
50. Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, A.10.4 : « Le Conseil des ministres insiste encore sur le fait que la Cour [Constitutionelle] a conclu au caractère disproportionné de l'atteinte au droit au respect de la vie privée par la loi du 30 juillet 2013 en raison de la combinaison de quatre éléments : le fait que la conservation des données concernait toutes les personnes, l'absence de différence de traitement en fonction des catégories de données conservées et de leur utilité, l'absence ou l'insuffisance de règles, ce qui constituerait une ingérence dans le droit à la protection de la vie privée. Or, ni la Cour de justice de l'Union européenne ni la Cour n'ont jugé que l'un de ces quatre éléments pouvait suffire à conclure au caractère disproportionné de la mesure. Le contrôle du principe de proportionnalité suppose en effet une approche globale. »↩
51. Cf. CJEU, *Tele2 Sverige AB/Watson, op. cit.* (n. 19), para 16.↩

52. Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) made on 31 October 2017 – *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (Case C-623/17), *O.J.* C 22, 22 January 2018, 29.↩
53. Request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018 — *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net v Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées* (Case C-511/18) and request for a preliminary ruling from the Conseil d'État (France) lodged on 3 August 2018, *French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs v Premier ministre, Garde des Sceaux, Ministre de la Justice* (Case C-512/18).↩
54. Request for a preliminary ruling from the Cour constitutionnelle (Belgium) lodged on 2 August 2018 — *Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v Conseil des ministres* (Case C-520/18).↩
55. Request for a preliminary ruling from the Supreme Court (Estonia) lodged on 29 November 2018 – *H.K. v Prokuratuur* (Case C-746/18).↩
56. Judgment of 6 October 2020, Case C-623/17, *Privacy International*, para 29.↩
57. Decrees (France) No 2015-1185, 2015-1211, 2015-1639 and 2016-67.↩
58. Law of 29 May 2016 amending, in particular, the loi du 13 juin 2005 relative aux communications électroniques, Moniteur belge of 20 June 2005, p. 28070; the code d'instruction criminelle and the loi du 30 novembre 1998 organique des services de renseignement et de sécurité, Moniteur belge of 18 December 1998, p. 40312. Cf. CJEU, 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *Quadrature du Net a.o.*, para 54.↩
59. Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, B.3. and B.4.1, also referring to Parl. Doc., Chamber, 2015-2016, DOC 54-1567/001, p. 6.↩
60. Constitutional Court of Belgium, Arrêt n° 96/2018 of 19 July 2018, B.4.2.↩
61. CJEU, *Privacy International*, *op. cit.* (n. 56), para 44 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 99.↩
62. CJEU, *Privacy International*, *op. cit.* (n. 56), para 43, 42 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 98, 97. See also above II.2.↩
63. Joined Cases C-511/18, C-512/18 and C-520/18 Quadrature du Net a.o., *op. cit.* (n. 58), para 99 and earlier judgments of 4 June 2013, Case C-300/11, *ZZ v Secretary of State for the Home Department*, para 38; of 20 March 2018, Case C-187/16, *Commission v Austria (State printing office),* para 75 and 76; and of 2 April 2020, Joined Cases C-715/17, C-718/17 and C-719/17, *Commission v Poland, Hungary and Czech Republic* (Temporary mechanism for the relocation of applicants for international protection), para 143 and 170.↩
64. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 99.↩
65. CJEU, *Privacy International*, *op. cit.* (n. 56), para 40, 41, thereby making reference to the definition provided in Art. 4(2) of Regulation 2018/679.↩
66. CJEU, 30 May 2006, Joined Cases C-317/04 and C-318/04, *Parliament v Council and Commission*, para 56-59. Please also see in the context of PNR the requests for preliminary rulings in the cases C-148/20, C-149/20 and C-150/20 (Lufthansa).↩
67. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, 31–50. This directive was repealed with effect of 25 May 2018 by Regulation 2016/679 (General Data Protection Regulation – GDPR).↩
68. CJEU, *Privacy International*, *op. cit.* (n. 56), para 46 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 101.↩
69. Ibid.↩
70. CJEU, *Privacy International*, *op. cit.* (n. 56), para 47 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 102.↩
71. CJEU, *Privacy International*, *op. cit.* (n. 56), para 48 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 103. See also to that effect Advocate General Saugmandsgaard Øe's opinion,*Ministerio Fiscal*, *op. cit.* (n. 48), para 47.↩
72. Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 January 2020 in the Joined Cases C-511/18 and C-512/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net* (C-511/18), para 65-76.↩
73. CJEU, *Parliament v Council and Commission*, *op. cit.* (n. 66), para 58.↩
74. CJEU, *Privacy International*, *op. cit.* (n. 56), para 82 and CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 168.↩
75. Ibid.↩
76. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 109, 113.↩
77. Ibid, para 115-117.↩
78. Ibid, para 118.↩
79. Ibid, para 125.↩
80. Ibid, para 125.↩
81. Ibid, para 126.↩
82. Ibid, para 128.↩
83. Ibid.↩
84. Ibid, para 130, 131.↩
85. Ibid, para 132, 133.↩
86. CJEU, *Tele2 Sverige AB/Watson*, op. cit. (n. 19), para 119.↩
87. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 135.↩
88. CJEU, *Tele2 Sverige AB/Watson*, op. cit. (n. 19), para 119.↩
89. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 136.↩
90. Ibid, para 139.↩
91. Ibid, para 146.148.↩
92. Ibid, para 152.↩
93. Ibid.↩
94. Ibid, para 153.↩

95. Ibid, para 154.↩
96. Ibid, para 155.↩
97. Ibid.↩
98. Ibid.↩
99. Ibid, para 157 and CJEU, 2 October 2018, Case C-207/16, *Ministerio Fiscal*, para 40 and 59.↩
100. Ibid, para 140, 157 and CJEU, *Ministerio Fiscal*, *op. cit.* (n. 99), para 62.↩
101. Op. cit. (n. 99).↩
102. Ibid, para 49.↩
103. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 159, 131, 158.↩
104. Ibid, para 140, 157.↩
105. Ibid, para 159.↩
106. Ibid.↩
107. Art. 2 lit. (g) of the e-Privacy Directive states:'value added service' means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof. Pursuant to Arts. 6 and 9 of that Directive data related to value added services may be processed to the extent and for the duration necessary for such services, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers may withdraw their consent at any time.↩
108. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 161.↩
109. Convention on Cybercrime of 23 November 2001 (European Treaty Series – No. 185).↩
110. Cf. Arts. 14 and 16 of the Convention on Cybercrime.↩
111. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 164.↩
112. Not necessarily national competent authorities, which hence might also apply to the European Public Prosecutor's Office.↩
113. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 163, 164.↩
114. The CJEU does not demand a prior review by a court or an independent administrative body.↩
115. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 164. Art. 16(2) of the Convention on Cybercrime also allows for a renewal of a preservation order and considers a period of time as long as necessary, up to a maximum of ninety days.↩
116. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 165.↩
117. Ibid, para 160.↩
118. Ibid, para 165.↩
119. See above under III.2.c) aa).↩
120. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 172.↩
121. Ibid, para 173.↩
122. Ibid, para 177.↩
123. Ibid, para 176-179.↩
124. Ibid, para 181.↩
125. Ibid, para 182.↩
126. Ibid. Cf. to that end also CJEU, Opinion 1/15 of 26 July 2017, *EU-Canada PNR Agreement*. This agreement stipulated in its Art. 26(2):"The Parties shall jointly review the implementation of this Agreement one year after its entry into force, at regular intervals thereafter, and additionally if requested by either Party and jointly decided."↩
127. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 183.↩
128. Ibid, para 184-185 and Article L. 851-4 of the French Code de la sécurité intérieure.↩
129. Ibid, para 187.↩
130. Ibid, 188.↩
131. Ibid, 189.↩
132. Ibid, para 66.↩
133. Ibid, para 38, 39, 66, 67.↩
134. Ibid.↩
135. Ibid.↩
136. Ibid, para 67.↩
137. Ibid, para 190.↩
138. Ibid.↩
139. Ibid, para 190.↩
140. Ibid, para 191.↩
141. Ibid, para 166.↩
142. Ibid.↩
143. Ibid.↩
144. CJEU, *Tele2 Sverige AB/Watson, op. cit.* (n. 19), para 120.↩
145. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 189 and CJEU, 2 March 2021, Case C-746/18, *H.K v Prokuratuur,* para 51 and 58, compared to the CJEU's judgement in *Tele2 Sverige AB/Watson*, *op. cit.* (n. 19), para 120.↩
146. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 176 and 189.↩
147. *Op. cit.* (n. 145).↩

148. H.K. was found guilty of the commission, within a period of around one year, of a number of thefts of goods of a value of 3 EUR to 40 EUR, thefts of cash of a value between 5.20 EUR and 2100 EUR, use of another person's bank card and acts of violence against persons, who were party to the court proceedings against her.↩
149. CJEU, *H.K v Prokuratuur, op. cit.* (n. 145), para 27-29.↩
150. Ibid, para 29↩
151. Ibid, para 30.↩
152. Ibid, para 31.↩
153. Ibid, para 32.↩
154. Ibid, para 33.↩
155. Ibid, para 35.↩
156. Ibid, para 35.↩
157. Ibid, para 46.↩
158. Ibid, para 47.↩
159. Ibid, para 48.↩
160. Ibid, para 49,50.↩
161. Ibid, para 52.↩
162. Ibid, para 54 and the cited case law.↩
163. Ibid, para 55.↩
164. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), , para 79 and 213.↩
165. Ibid.↩
166. Ibid.↩
167. Ibid, para 214-218. The CJEU stated that the national court may exceptionally maintain the effects of a measure despite a breach of procedural rules, where it is justified by overriding considerations to nullify a genuine and serious threat, such as the interruption of the electricity supply in the Member State concerned, cf. CJEU, 29 July 2019, Case C-411/17, *Inter-Environment Wallonie and Bond Beter Leefmilieu Vlaanderen*. The CJEU, however, further stressed that this exception does not apply in the case at hand, as the legislation under review would continue to impose obligations on service providers which are contrary to EU law and which seriously interfere with fundamental rights (para 219).↩
168. Ibid, para 222.↩
169. Ibid, para 223.↩
170. Ibid, para 223 and case law cited.↩
171. Ibid, para 225.↩
172. Ibid, para 226.↩
173. Ibid, para 226 and the case law cited.↩
174. Ibid, para 228.↩
175. CJEU, 10 April 2003, Case C-276/01, *Joachim Steffensen*.↩
176. ECtHR, 18 March 1997, *Mantovelli v France*, Appl. No. 21497/93.↩
177. CJEU, *Steffensen*, *op. cit.* (n. 175), para 52.↩
178. ECtHR, *Mantovanelli v. France, op. cit.* (n. 176), para 36.↩
179. ECtHR, 12 July 1988, *Schenk v. Switzerland*, Appl. no. 10862/84, para 45-46; ECtHR [GC], 11 July 2017, *Moreira Ferreira v. Portugal* (no. 2), Appl. no. 19867/12 , para 83; ECtHR, 1 March 2007, *Heglas v. the Czech Republic*, Appl. no. 5935/02, para 84.↩
180. ECtHR, 27 October 2020, *Ayetullah Ay v. Turkey*, Appl. nos. 29084/07 and 1191/08, para 123- 130.↩
181. ECtHR [GC], 1 June 2010, *Gäfgen v. Germany,* Appl. no. 22978/05, para 164.↩
182. This concerns, for instance, cases related to the use of evidence obtained by unlawful secret surveillance (ECtHR cases *Bykov v. Russia* [GC], para 69-83; *Khan v. the United Kingdom*, para 34; *Dragojević v. Croatia*, para 127-135; *Niţulescu v. Romania*; *Dragoş Ioan Rusu v. Romania*, para 47-50), and search and seizure operations (ECtHR cases *Khodorkovskiy and Lebedev v. Russia*, para 699-705; *Prade v. Germany*; *Tortladze v. Georgia*, para 69, 72-76, concerning the search of the premises of an honorary consul; *Budak v. Turkey*, para 68-73 and 84-86, concerning, in particular, the importance of examining the issues relating to the absence of attesting witnesses.↩
183. Cf. e.g. the decision by the German *Bundesgerichtshof* (Federal Court) concerning the use of retained data as evidence in criminal proceedings in the context of the retention law being declared as unconstitutional by the German *Bundesverfassungsgericht* (Federal Constitutional Court), BGH, 4. November 2010 - 4 StR 404/10.↩
184. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 137.↩
185. Ibid, para 135.↩
186. Ibid, para 139.↩
187. Ibid, para 135.↩
188. Ibid, para 142.↩
189. Ibid, para 149.↩
190. Conseil d'Etat (France), decision in cases Nos. 393099, 394922, 397844, 397851, 424717, 424718 of 21 April 2021, para 53.↩
191. Ibid, para 54.↩
192. See also Milieu, "Study on the retention of electronic communications non-content data for law enforcement purposes", Publications Office of the EU (europa.eu), September 2020 (published on 7 December 2020 [ISBN: 978-92-76-22841-7]), § 9.2.2, p. 113.↩
193. Conseil d'Etat (France), *op. cit.* (n. 190), para 53.↩
194. Center for Democracy & Technology: <https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf> accessed 9 August 2021.↩

195. Cf also CJEU, *Digital Rights Ireland and Seitlinger a.o.*, *op. cit.* (n. 9), para 60.↩
196. CJEU, *Ministerio Fiscal*, *op. cit.* (n. 99), para 56.↩
197. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *O.J.* L 335, 17.12.2011, 1.↩
198. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 154.↩
199. CJEU, *Privacy International*, *op. cit.* (n. 56), para 154, and above under III. 2. c)cc).↩
200. Ibid, para 154.↩
201. See also the Milieu study, *op. cit.* (n. 192) , § 9.2.2, p. 113, § 5.2, p. 52.↩
202. To be found under <https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption> accessed 9 August 2021.↩
203. See for an overview of the data categories proposed in the e-evidence Regulation: <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345> accessed 9 August 2021.↩
204. Art.18 of the Convention on Cybercrime, *op. cit.* (n. 109).↩
205. CJEU, *Quadrature du Net a.o.*, *op. cit.* (n. 58), para 154, 161.↩
206. Ibid, para 163-164.↩
207. Cf. also the Milieu study, *op. cit.* (n. 192), section 7.5.↩
208. Cf. also Max-Planck-Institut für ausländisches und internationales Strafrecht, "Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten", July 2011, p. 227.↩
209. Milieu, *op. cit.* (n. 192), section 7.5.2.↩
210. According to a report by the Swiss journalist Timo Grossenbacher, two out of three persons are wrongly suspected by the software used by the Swiss Police, *SRF* <https://www.srf.ch/news/schweiz/predictive-policing-polizei-software-verdaechtigt-zwei-von-drei-personen-falsch> accessed 9 August 2021.↩
211. On related questions of handling algorithms in the work of the police and judicial authorities, cf. M. Simmler, S. Brunner and K. Schedler, "Smart Criminal Justice – Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege", 2020, University of St. Gallen, available at: <https://www.alexandria.unisg.ch/261666/> accessed 9 August 2021.↩
212. Proposal of 10 January 2017 for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.↩
213. See for more background: <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform> accessed 9 August 2021.↩
214. COM(2017) 10 final, *op. cit.* (n. 212), §1.3 "Consistency with other Union policies".↩
215. <https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html> accessed 9 August 2021.↩
216. See T. Wahl, "Council Agrees on Negotiating Mandate for E-Privacy Regulation – Data Retention Included", (2021) *eucrim*, 30; Council doc. 6087/21 of 10 February 2021.↩
217. Progress report of the German Presidency to the Council of the EU, ST 13106/20 of 23 November 2021.↩
218. Cf. CJEU, 7 May 2013, Case C-617/10, *Åkerberg Fransson*.↩
219. Cf. <https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/ePrivacy_Verordnung.html> accessed 9 August 2021.↩
220. Max-Planck-Institut für ausländisches und internationales Strafrecht, "Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten", July 2011.↩
221. Ibid, p. 218.↩
222. Ibid, p. 221.↩
223. Study of the Legal Service of the European Parliament - General data retention / effects on crime, 10 December 2019.↩
224. Ibid, p. 3.↩
225. Milieu Study, *op. cit.* (n. 192).↩
226. Ibid, p. 14-15. The limitations of the study are that the sample of replies is not statistically representative for all law enforcement authorities and electronic communications service provider(s) in the 10 Member States and data gaps exist due to the reluctance (or inability) of stakeholders to share information on data retention; furthermore, comparability of the data collected is limited, given the differences in national definitions and practices.↩
227. See e.g. Art. 42 on judicial review of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office, *O.J.* L 283, 31.10.2017, 1.↩
228. CJEU, 12 November 1969, Case C-29/69, *Erich Stauder v Stadt Ulm*.↩
229. Similarly, E. Tuchtfeld, "Towards a European Court of Fundamental Rights, How the European Court of Justice Becomes a Last Instance of Fundamental Rights Adjudication in Europe", *Verfassungsblog*, 19. October 2020 <https://verfassungsblog.de/towards-a-european-court-of-fundamental-rights/> accessed 9 August 2021.↩
230. CJEU, 14 February 2008, Case C-450/06, *Varec,* para 48; CJEU, 9 November 2010, Joined Cases C-92/09 und C-93/09, *Schecke GbR and Eifert v Land Hessen,* para 53.↩
231. Cf. Request for a preliminary ruling from the Bundesverwaltungsgericht (Germany) lodged on 29 October 2019 — *Federal Republic of Germany v SpaceNet AG,* (Case C-793/19) and *Federal Republic of Germany v Telekom Deutschland GmbH* (Case C-794/19); request for a preliminary ruling from the Cour Cnstitutionnelle (Belgium) lodged on 31 October 2019 — *Ligue des droits humains v Conseil des ministers* (Case C-817/19); reference for a preliminary ruling from the Supreme Court (Ireland) made on 25 March 2020 — *G.D. v The Commissioner of the Garda Síochána, Minister for Communications, Energy and Natural Ressources, Attorney General* (Case C-140/20); request for a preliminary ruling from the Cour de cassation (France) lodged on 24 July 2020 — *VD* (C-339/20) and 20 August 2020 — *SR* (Case C-397/20).↩
232. Conseil d'Etat (France) Decision in cases Nos 393099, 394922, 397844, 397851, 424717, 424718 of 21 April 2021 and Constitutional Court (Belgium) case nr. 57/2021 of 22 April 2021.↩

233. Opinion of Advocate General *Campos Sánchez-Bordona*, 18 November 2021, Joined Cases C-793/19 *SpaceNet* and C-794/19 *Telekom Deutschland*, Case C-140/20 *Commissioner of the Garda Siochana and Others*, and Joined Cases C-339/20 *VD* and C-397/20 *SR*. It is of note that the latter joined cases concerned particularly the relation between specific Union legislation on insider dealing, market manipulation and market abuse and the e-Privacy Directive as far as access to traffic and location data is concerned.↩
234. Opinion in *SpaceNet, op. cit.* (n. 233), para 41.↩
235. Opinion in *VD* and *SR, op. cit.* (n. 233), para 85, 86.↩
236. Opinion in *SpaceNet, op. cit.* (n. 233), para 43-50.↩
237. Opinion in *SpaceNet, op. cit.* (n. 233), para 83.↩
238. Cf. the requests cited in n. 231.↩

Authors statement

The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union